GDPR Report Dated: 12/07/2018

HTR School

Headteacher's Name	Neil Jones
URN	999999

Use this area to add the data background, action plan and the IT context for your school, for example:

IT and Data SLA provided by School IT R Us who provide all IT service, support and external back-ups of school information.

We have identified all third parties who we share pupil, staff or parent data with and are working with them to ensure GDPR compliance.

The DPO will update the SLT and Governors termly with any GDPR actions.

Key Information

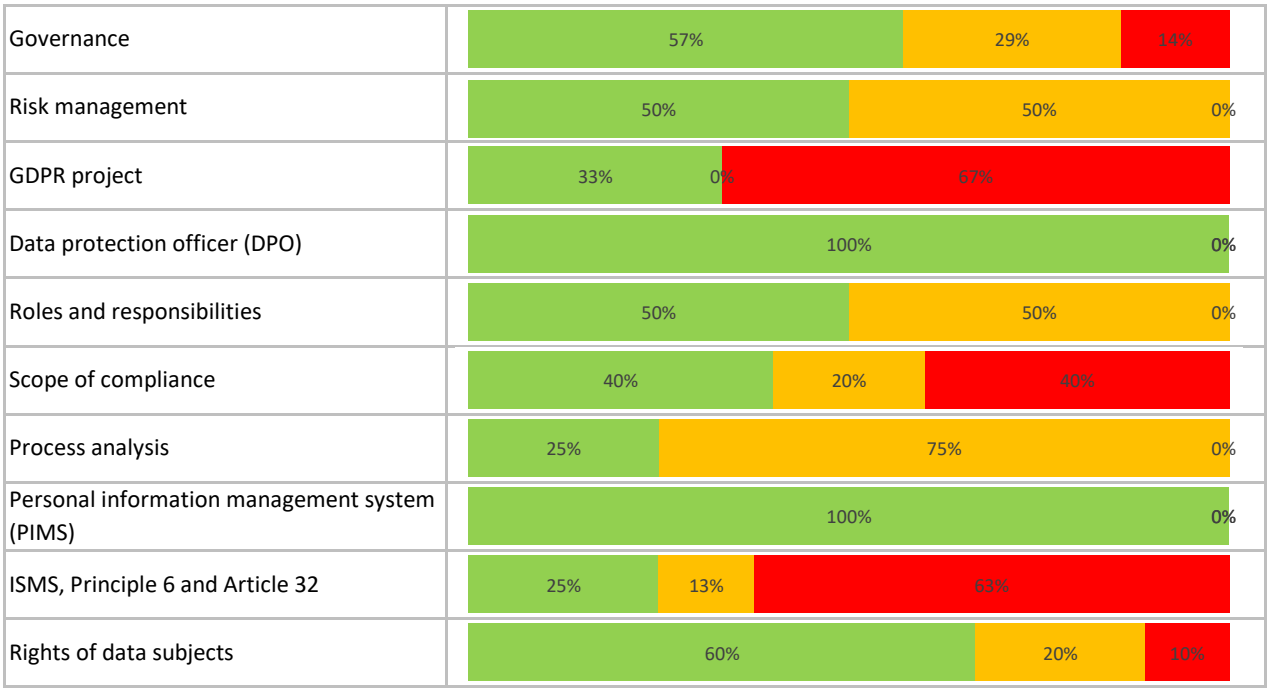
Data Protection Lead	Hannah Charlton
Data Protection Officer	Matt Birch
Date of last GDPR Review	12 July 2018

Executive Summary

Review date 12 July 2018

Overall GDPR conformance

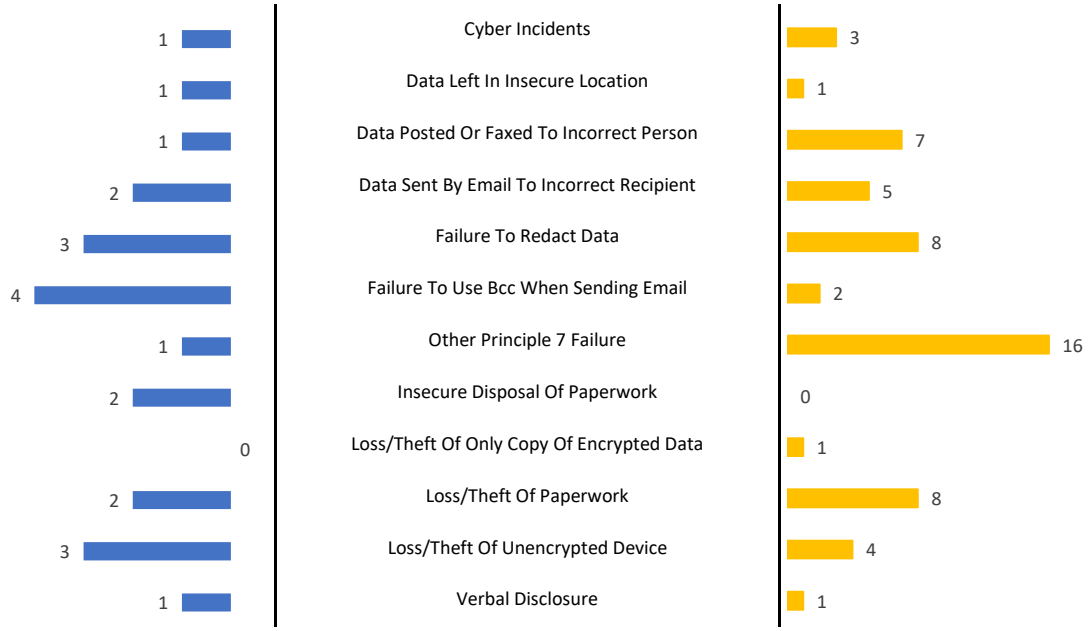
Compliance by section



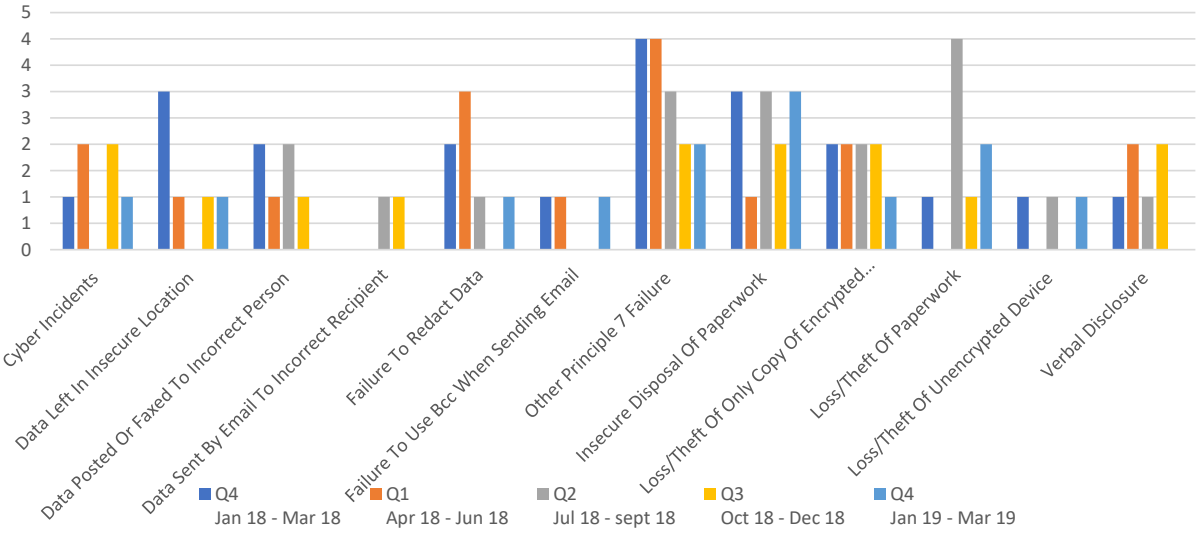
Number of freedom of information requests since the last report	2
Number of data security incidents reported in total since the last report	4
Number of data security incidents reported to the ICO in total	1
Have the governors been made aware of any reported incidents and what the outcome / impact was?	Yes
Number of third party organisations the school shares data with	10
Are all third party organisations GDPR compliant (see separate checklist)?	No
Number of subject access requests since the last report	0

Quarterly data: Data protection incidences and trends - Reported to the ICO

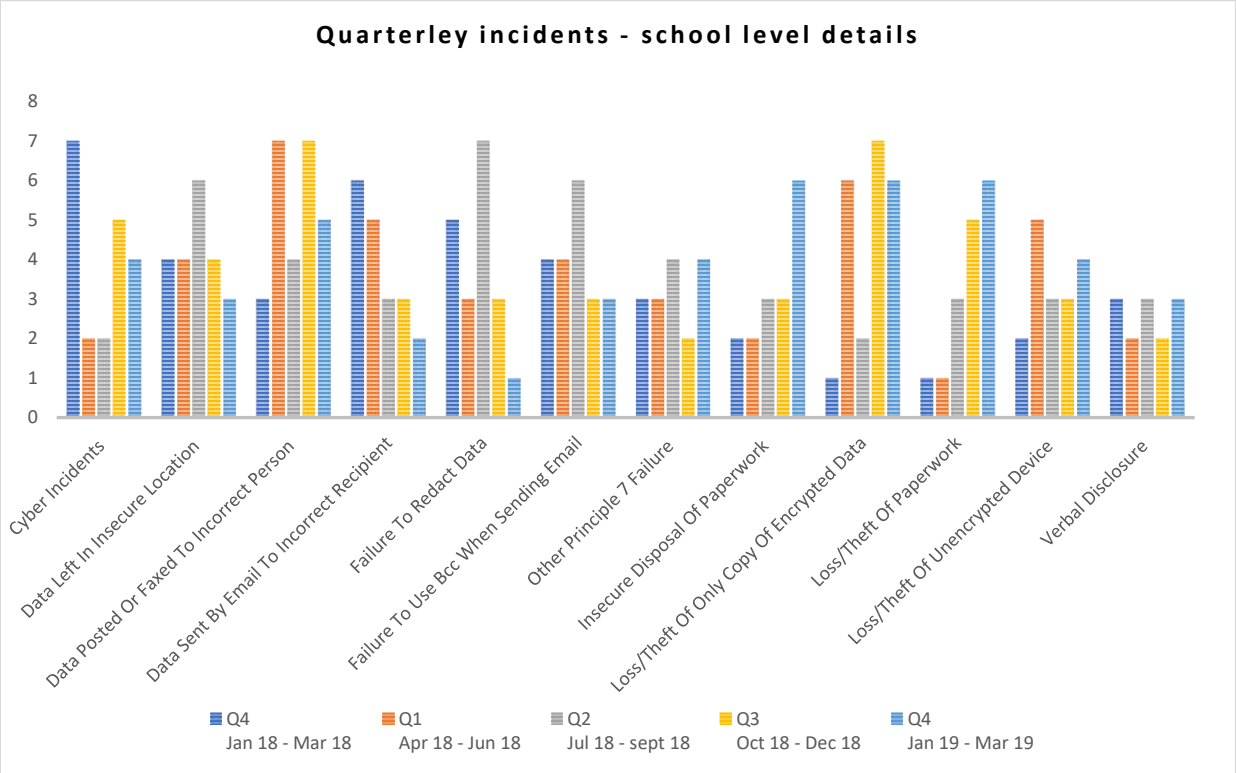
School Level Incidents	Total national education reported incidents
Q4 Jan 18 - Mar 18	Q4 Jan18 - Mar18 (National)



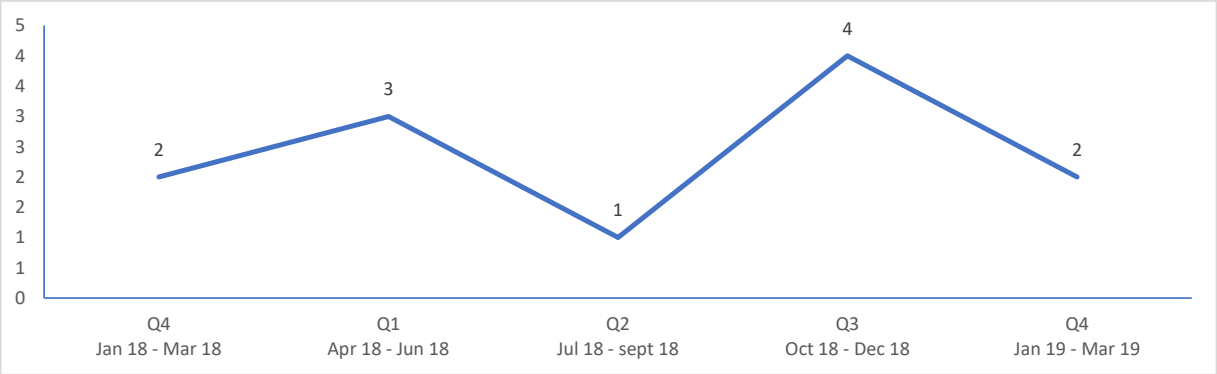
School level quarterly security incidents and trends



Quarterly data: Data protection incidences and trends - Total Incidents



Quarterly Subject Access Request - School Level



Data Protection and the GDPR - Termly Audit

Review Date 12/07/2018

Please note: the audit responses are completed by the school and cannot guarantee GDPR compliance

1. Governance	Reponses
There is awareness and understanding of the need to address GDPR with the following?	
Governing Body/Trust Board	Yes
Headteacher/Executive Headteacher/Principal	In-Part
Wider Senior Leadership Team	No
Middle Leaders	Yes
DPA/GDPR compliance oversight	
The Governing Body has an accountable Senior Leader	In-Part
The DPA/GDPR is on Governing Body and SLT meeting agenda	Yes
The Governing Body receives regular audit reports on GDPR compliance	Yes
2. Risk management	
The school has a risk register	In-Part
GDPR risk (fines and legal actions) is on the school's risk register	In-Part
Privacy risk (to data subjects) is on the school's risk register	In-Part
The risk framework includes a method for assessing both these forms of risk	Yes
The internal control framework includes privacy risk	Yes
The internal audit programme includes GDPR compliance	Yes
3. GDPR project	
There is a GDPR Project Team	Yes
It has Senior Leadership support	Yes
It has a clear plan	No
The planned deliverables can be achieved	No
There are adequate project resources	No
The Project Team has the necessary knowledge and training	No

4. Data protection officer (DPO)	
A Data Protection Officer has been appointed	Yes
Their reporting arrangements meet the requirements	
Independence	Yes
Direct access to Senior Leadership	Yes
Adequately resourced	Yes
Competent (knowledge of the GDPR)	Yes
Informed (and up-to-date with current developments)	Yes
Knowledgeable about cyber security	Yes
The level of responsibility meets the Privacy Compliance Framework (PCF)?	Yes
5. Roles and responsibilities	
There are colleagues who have responsibilities for personal data within	
Administration and Finance Team	Yes
Teaching Staff and other Classroom Staff	Yes
IT/Network Staff	Yes
Catering Staff	Yes
The GDPR is included in the staff induction	
Permanent Staff	In-Part
Supply/Temporary Staff	In-Part
There is a mandatory GDPR staff awareness programme	In-Part
All staff have completed it	In-Part
6. Scope of compliance	
The scope of the Privacy Compliance Framework is identified	In-Part
The legal entity is identified	In-Part
Personal data is only collected within the EU	Yes
Personal data is only stored or processed within the EU	Yes
Interfaces, third parties, hand-offs (see supply list page for a breakdown)	
Third-parties that might share data have all been identified	Yes
GDPR-compliant contracts are in place to cover data processing aspects	Yes
Cloud providers have been identified	No
The status of these relationships has been identified	No
GDPR-compliant contracts are in place for Cloud-based data processing	No
Are all these relationships inside of the EU?	No

7. Process analysis	
Processes that handle personal data have been reviewed to assess risk	Yes
Risks have been mitigated, removed or accepted	Yes
Does any processing mandate a Data Protection Impact Assessment (DPIA)?	
Large-scale processing	In-Part
Development of new systems	In-Part
Processing of sensitive data, e.g. biometrics or health data	In-Part
Does the DPO oversee all DPIA activity?	In-Part
Is the DPIA process part of the project planning process?	In-Part
Are any IT or system projects commencing/commenced that require a DPIA?	In-Part
8. Personal information management system (PIMS)	
Consent processes are documented	
The process for gathering consent to process is GDPR compliant	Yes
A process for gathering the consent of over 13s has been introduced	Yes
There is an appropriate mechanism for withdrawal of consent	Yes
The processing of employee data has been shifted away from consent within contracts	Yes
Data relating to under 13s has been reviewed & includes parent consent	Yes
Article 13 privacy notices are published	Yes
Article 14 privacy notices are issued	Yes
Documentation has been updated	Yes
The organisation has documented its data processing activities (Article 30.)	Yes
The data protection policy has been updated	Yes
There is a data subject access request process	Yes
The data subject access request process is effectively implemented	Yes
These policies and procedures have been updated	
Retention schedule	Yes
Access provisioning on a need-to-know basis	Yes
Records management	Yes
Data classification	Yes
Bring Your Own Device (BYOD)	Yes
Change management (does it link to review of DPIA?)	Yes
Retention schedule and policy	Yes
A list of databases likely to contain data beyond the lawful retention date	Yes
An incident response process	Yes
A data breach reporting process	Yes
A contract management process (SLAs, security etc)	Yes

9. Information security management system (ISMS), Principle 6 and Article 32	
Encryption and Pseudonymisation	
There is an encryption policy (FIPS 140-2)	Yes
Mobile devices are encrypted	In-Part
Databases are encrypted	No
External storage devices are blocked/encrypted	No
Email is encrypted	No
Pseudonymisation is deployed	No
Information Security	
There is regular external network penetration testing	No
There is regular internal network penetration testing	Yes
Websites/applications are regularly security tested	Yes
There is an information security policy	Yes
The information security policy references security of data subjects	No
Frameworks and standards implemented	
Cyber Essentials	No
Cyber Essentials Plus	No
BS10012	No
ISO 27001	No
PCI DSS - if your school takes card payments	In-Part
10. Rights of data subjects	
The school facilitates the exercise of data subjects' rights	In-Part
The school has procedures and technologies in place that enable it to respond to exercise of:	
Right to be informed	Yes
Right of access	Yes
Right to rectification	Yes
Right to erasure	Yes
Right to restrict processing	Yes
Right to data portability	Yes
Right to object	No
Rights in relation to automated processing and profiling	In-Part