



GDPR & Education part 2

Vertical Structure - Prepare, Protect, Persist®



- Prepare
 - We help you and your partners to understand how to identify and resolve potential security issues at the earliest stages with hands on 'hack yourself first', threat modelling and GDPR compliance workshops as well as security training for non-technical colleagues.
- Protect
 - Using automated and manual penetration testing techniques, we provide a comprehensive security report for your Web and mobile applications, including API testing, and networks. The report highlights potential issues and their resolutions.
- Persist
 - We ensure that your organisation benefits from continual improvements in security levels through information assurance processes, auditing and certification including ISO27001:2013 and Cyber Essentials.



Simon Whittaker

- Parent Governor at Holywood Nursery School & St Patrick's Primary School
- Security consultant/tester



GDPR – some of the details

- What is it?
- When does it come into effect?
- Small organisations
- GDPR in Education
- What do I need to do?



Disclaimer

- This is not meant as a substitute for legal advice on particular issues and action should not be taken on the basis of the information in this document alone.
- Vertical Structure Ltd make no warranty, representation or guarantee, express or implied, as to the information contained.



What is it?

- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
 - Enacted in the UK as Data Protection Act 2018
 - Replacement for the 1995 Data Protection Directive
 - Officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
 - Enacted in the UK as the Data Protection Act 1998
 - Basic compliance required registration with the ICO in the UK
- Designed to help protect personal data
- Legislating common sense

What was wrong with the Data Protection Act?



- Designed for 1998 not 2018
- No understanding of current world:
 - Distributed Web Applications
 - Cloud Environments
 - Big Data including:
 - Sharing across borders
- Enforcement tends to be on self-reported incidents
 - Large amount of fines for charities and public bodies
- Inconsistencies across member nations



When did it come into effect?

- Enforced from 25th May 2018



- *“GDPR is an evolution in data protection, not a total revolution. GDPR is building on foundations already in place for the last 20 years.”*
 - Steve Wood – Deputy Commissioner for Policy, ICO
- Evolution yes but also revolution

GDPR & small organisations – does this even apply to me?



- Article 30 of the regulation declares that:

The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons



Unless.....

- The processing it(the organisation) carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9, or personal data relating to criminal convictions and offences referred to in Article 10.
- In addition, if a company's processes deal routinely with personal data, then that company should abide by the regulation.



Basically

- Yes
- As a rule of thumb, ICO has stipulated that **any business which is affected by the Data Protection Act (DPA)** will also be affected by the GDPR.
- The GDPR should, in fact, be seen as an enhanced version of the UK's own DPA.



Some important points

- What counts as personal data/sensitive personal data?
- Data processor vs data controller
- Lawful Basis for Processing
- Rights of the data subject
- Data defence
 - Why do you have this data?
- Data portability
 - Subject Access Requests
- Breach notification
- Passing on of data to someone else
- Territoriality
- Enforcement



Definitions

- Data Subject
 - A natural person
 - A citizen or resident of an EU member state
- Data Controller
 - Organisation that collects data
 - Responsible for determining the purposes, condition and means of processing personal data
- Data Processor
 - Processes data on behalf of data controller
 - Service provider like a **hosting provider** or **cloud provider**
 - DP can now be subject to direct enforcement



What counts as personal data?

- Any information relating to an identified or identifiable natural person (the data subject) – this is just a sample of what **could** be personal data
 - Name
 - Birthdate
 - Address
 - Mobile device id
 - Social media posts
 - Photos
 - IoT collected data
- Personal data is owned **by the individual**, not the organisation holding it
- Paper and electronic are just as valid – if the data is **organised**

Sensitive personal/Special Category data



- Race;
- Ethnic origin;
- Politics;
- Religion;
- Trade union membership;
- Genetics;
- Biometrics (where used for ID purposes);
- Health;
- Sex life; or
- Sexual orientation.



Lawful Basis for Processing

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interests





Consent

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

- Data must be freely given - Data subject **must** be able to say no
- The consent must be specific and intelligible - what **exactly** is the processor doing
- Informed – all purposes the data will be used for.
- Consent must be unambiguous - “clear affirmative action” to signify consent

Consent for sensitive data & Children's data



- Must be explicit
 - “yes, I agree to my sensitive personal data to be used as described ‘here’”
- Where the child is below the age of 16 years such processing will be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child
- Processing only able to be performed if consent provided by the parent(this can change depending on location – can be between 13-16)



Consent for pictures

- *[Example 4] A public school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.*



Photos and the DPA 2018

- The Data Protection Act is unlikely to apply in most cases where photographs or videos are taken in schools and other educational institutions.
- If photos are taken for personal use they are not covered by the Act.
- Photos taken for official school use may be covered by the Act, so pupils and students should be advised why they are being taken.



Personal Use

- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.
- Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.



Official Use

- Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.
- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.



Media Use

- A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.



Correct lawful basis for processing

- Consent is not always best basis
- Contract
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interests



Consent vs Legitimate Interest

The processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data...

The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. (Recital 47)

- If you want to use the legitimate interest condition then you should:
 - Consider your rationale carefully
 - Be able to justify it – document it!
 - Demonstrate that you aren't overriding an individual's rights
 - Consider if processing the data to send direct marketing is within their reasonable expectations.
- Institute of Fundraising have a great guide
 - <http://vsLtd.co/iofGDPRGuide>

The right to erasure/right to be forgotten



- The data subject may request erasure of their data when there is no compelling reason for it to be retained
 - Must be erased if they withdraw consent
 - Must be erased if they request it
 - Not an absolute right to erase
 - Must be erased if found to be in breach
 - Only be used for the purposes for which it was given



Right to erasure

"I want my child school history deleted"

"I want my employment history deleted"

	Right to Erasure	Right to Portability	Right to Object
Consent	✓	✓	✗
Contract	✓	✓	✗
Legal Obligation	✗	✗	✗
Vital Interests	✓	✗	✗
Public Task	✗	✗	✓
Legitimate Interests	✓	✗	✓

Data Defence – why do we need this data?



“personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”

- Don't collect data you don't actually need
- Is birthdate a required field when purchasing something from an online store?
 - Why?
- How long do we store it?
 - Backups
 - Spreadsheets
- Where do we store it?
 - CRM systems
 - Spreadsheets
 - Laptops – encrypted?
- Why are we retaining it?

The screenshot shows a Twitter thread. At the top, user **szlwzl** (@szlwzl) asks **@hm_custserv** why they need a birthdate to buy clothes. The tweet is from July 23, 2017. Below it is a text box for replying. The thread continues with a reply from **H&M Customer Service** (@hm_custserv) on July 24, stating they have age restrictions. **szlwzl** then asks if the information is retained for processing. A final reply from **H&M Customer Service** on July 24 explains they keep birthdates for data protection purposes.

The right to be informed & Subject Access Requests



- The data subject may obtain confirmation that their data is being processed and gain access to the data itself
- Must be free
- Can charge for multiple identical requests but only limited cost.

“.....where the request is manifestly unfounded or excessive you may charge a “reasonable fee” for the administrative costs of complying with the request.”

Subject Access Request



© 2018 Vertical Structure Ltd

Time to comply with Subject Access Requests



“You must act on the subject access request without undue delay and at the latest within one month of receipt.”

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>



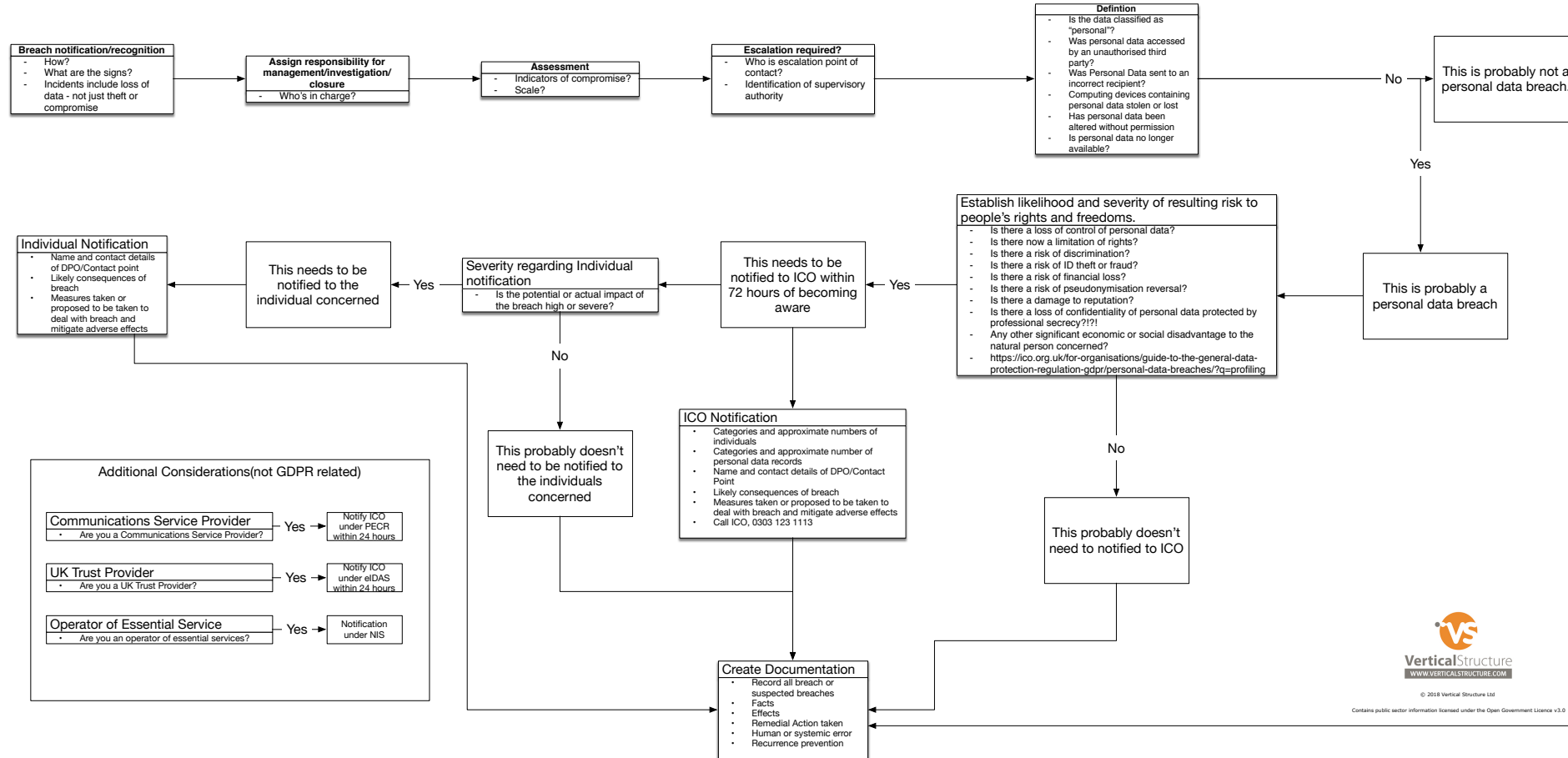
Breach Notification

Under the Data Protection Act (DPA), although there is no legal obligation on data controllers to report breaches of security, we believe that serious breaches should be reported to the ICO.

<https://ico.org.uk/for-organisations/report-a-breach/>

- Under GDPR:
 - Breaches of personal data need to be reported as soon as possible (if within certain criteria)
 - Ideally within 24 hours
 - Certainly within 72 hours
- Must be clear about:
 - What's been lost
 - How it happened
 - Potential impacts
 - Mitigations which you've done

Breach Notification Process





Record Keeping

Each controller, and where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.

- Who is the controller?
 - Name/contact details
- Purpose of processing
- Categories of data subjects AND categories of personal data being stored.
- Is any of the data listed as “sensitive”
- Who are recipients of the data?
- Any transfers to another country or international organisation
- Time limits for erasure
- Technical & organisational security measures in place



CCTV – what should I know?

- Guidance is confused and confusing
- ICO recommend following guidance from Protection of Freedoms Act(POFA)
- Data captured using CCTV can be requested under a subject access request
 - Removal of personal data belonging to others may be required
- ICO guidance suggests conducting a “Privacy Impact Assessment”
 - Helps assess requirement for CCTV
 - Could a less intrusive method be used?



CCTV disclosure

- Schools may disclose CCTV footage relating an individual:
 - With third parties who are directly involved in dealing with any request, enquiry, complaint or other correspondence submitted by an individual which the footage is relevant to;
 - With third parties who are providing a school with professional advice which the footage is relevant to where necessary for their legitimate interests and permitted by law;
 - Where a school is legally required to do so;
 - In connection with criminal investigations, legal proceedings or prospective legal proceedings which the footage is relevant to for the related legitimate interests of a school or a third party and permitted by law;
 - In order to establish, exercise or defend a school's legal rights where necessary for their legitimate interests and permitted by law; and
 - Where a school has stated or informed an individual otherwise.



CCTV steps to take

- Governance
 - Do we actually need this?
- Storage
 - How do we protect the data?
- Openness and honesty
 - Tell people that they are being surveilled
 - Tell people who is responsible for the system
- Disclosure and Subject Access Requests
 - Who can disclose?
 - When can it be disclosed?
 - Technical measures?



CCTV steps to take

- Retention
 - How long do we need this data for?
- Selecting and siting surveillance systems
 - Reduce the impact on general public and others
 - Can public spaces be blocked
- Using the equipment
 - Access to control room
 - Quality of images
 - Encryption
- Create a policy



Level 2 – Checklist for CCTV

Define the Problem



Operational Issues (Live Viewing)



System Requirements

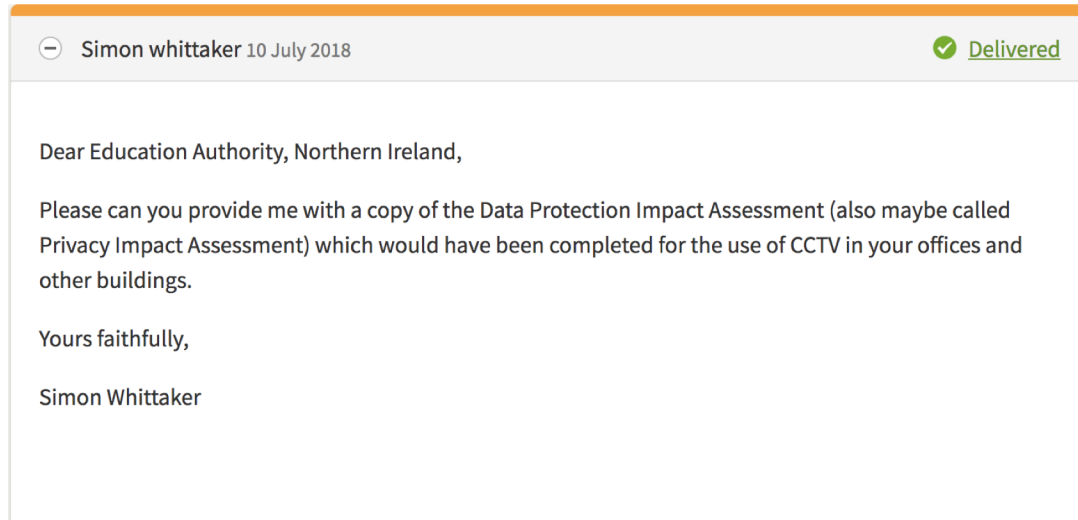


Management Issues



NICS CCTV report 2016

Asking the questions




The Education Authority is currently reviewing its policies and procedures around the use of CCTV in all of its premises as part of the Authority's GDPR Implementation Programme. Under the provisions of Article 35 of the GDPR and Recital 91 in conjunction with the recommendations contained in the 'Draft Guidance on DPIA's' issued by the Information Commissioners Office, it is envisaged that DPIA will be completed in respect of CCTV operations and made available to the public via the Authority's publications scheme.

It should be noted however that all schools are registered with the Information Commissioners Office as independent Data Controllers in their own right via their Data Protection Notification and as such are responsible for DPIA's in relation to their own CCTV systems.

https://www.whatdotheyknow.com/request/data_protection_impact_assessmen



3 cameras in the same place looking the same way	A mobile CCTV camera	A free standing camera	A camera in a cage
Camera linked to a monitor you can see yourself on	A shiny camera with spikes on	A camera that makes you wonder why it is there	A camera that looks like a spaceship
A place you are glad to see a camera	A camera that turns when you look at it	A subverted or vandalised camera	A camera that is trying to hide from you
A ridiculous camera	A camera that isn't there but you wish it was	A very high up camera	A camera that looks like a work of art
A camera with a bird sat on it	A camera that talks to you	360degree camera	A privately owned camera
A camera without an obvious owner	A strange looking camera		

Please share your findings with The LRM (Loiterers Resistance Movement).
 We are a Manchester based collective interested in psychogeography, public space, creative walking, DIY mapmaking and uncovering the hidden stories of our city. We believe the streets should belong to everyone, there is poetry in the pavements and magick in the manunian rain. On the First Sunday of every month we go for a free, communal wander of some sort and you would be very welcome to join us.
www.thelrm.org [twitter@thelrm](https://twitter.com/thelrm) [f.book loiterers resistance movement](https://www.facebook.com/loiterersresistancemovement) email mrose@thelrm.org
 Images by David Dunnico www.dunni.co.uk used with thanks. Cheers to all who walk with us.

Enforcement



ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home For the public For organisations Report a concern **Action we've taken** About the ICO

Action we've taken /

Enforcement action

Filters 207 in total

Type

- All
- Monetary penalties 90
- Undertakings 50
- Enforcement notices 37
- Prosecutions 30

Sector

- All
- Marketing 34
- General business 26
- Finance insurance and credit 20
- Local government 20
- Charitable and voluntary 18
- Health 14
- Online technology and telecoms 12
- Criminal justice 10

Home Logic UK Ltd
18 August 2017, Monetary penalties, Marketing
Domestic energy saving firm Home Logic UK Ltd has been given a £50,000 penalty...

Kent Police
18 August 2017, Undertakings, Criminal justice
A follow up has been completed to provide an assurance that Kent Police has appr...

London Borough of Islington
17 August 2017, Monetary penalties, Local government
Islington Council failed to keep up to 89,000 people's information secure on its par...

Brioney Woolfe
11 August 2017, Prosecutions, Health
A former employee of Colchester Hospital University NHS Foundation Trust, Brione...

Cheshire West and Chester Council
10 August 2017, Undertakings, Local government
An Undertaking to comply with the seventh data protection principle has been sign...

TalkTalk Telecom Group PLC
10 August 2017, Monetary penalties, Online technology and telecoms
The Information Commissioner's Office has fined TalkTalk Telecom Group PLC £10...

<https://ico.org.uk/action-weve-taken/enforcement/>

© Vertical Structure Ltd where applicable
simon.whittaker@verticalstructure.com



Enforcement

- Two tier system for infringements
 - Lesser incidents subject to a maximum fine of either €10 million (£7.9 million) or 2 per cent of an organisation's global turnover (whichever is greater)
 - Most serious violations could result in fines of up to €20 million or 4 per cent of turnover (whichever is greater)
- Fines will be:
 - Effective
 - Proportionate
 - Dissuasive
- Will take into account
 - Gravity & duration of the infringement
 - What did the organisation do to mitigate the damage?



Enforcement

- TalkTalk were breached in 2016 and faced a fine of £400,000 for security failings which made national news. This fine was 0.022% of gross revenue
- If proof of negligence and ongoing, consistent infringements this could have been ~£59million under GDPR.



Other Enforcements

- Issue warnings
- Reprimands
- Force controller to comply with data subject's requests
- Bring processing to compliance
- Tell a data subject about a breach
- Compel erasure
- Suspension of flows to a third country
- **“Stop Processing” (temporary or definitive limitation)**





Data Protection Officer

- Appointed by the company engaged in regular and systematic monitoring of individuals on a large scale” or who process data on a regular basis.
- They keep the Controller and Processor in check and one must be appointed **if** you:
 - Are a public authority (except for courts acting in their judicial capacity);
 - Carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
 - Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.



DPO's tasks

- Inform and advise you and your employees about your obligations to comply with the GDPR and other data protection laws
- Monitor compliance with the GDPR and other data protection laws, and with your data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits
- Advise on, and to monitor, data protection impact assessments
- Co-operate with the supervisory authority
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, children etc).



DPO

- Take into account risk to the organisation
- Prioritise and focus on the organisation's riskier activities
 - Special categories of data

What is the Education Authority doing?



“subject to consultation with the Information Commissioner’s Office, EA is prepared to assume the specific role of Data Protection Officer (DPO) for all schools...”

“Please email thinkdata@eani.org.uk if you would like EA to assume the DPO role for your school.”

Letter from EA - 27 April 2018



What do I need to do?

- Protection/Security by design
 - Think about security as you implement new systems
- Understand your data
- Use the resources available to you
 - <http://www.eani.org.uk/about-us/ea-think-data-online-resource-hub/templates-and-guides/>
- Read the FAQ and the Action Plan



Who, What, Why, When, Where?

Who

- Whose data is being held by the organization?

What

- What data is being held by the organisation

Why

- Why is the data being held

When

- When is the data deleted?

Where

- Where is the data held or stored?



GDPR Action plan

- Awareness
 - Inform staff and volunteers
- Register with the ICO
- Fill in the Information Asset Register
- Update privacy notices
- Update data protection policy
- Ensure individuals are aware of their rights



GDPR Action plan

- Review consent
- Special emphasis on Children's data and special category
- Understand data breaches and what you would do
- Develop processes which use privacy by design
- Use Privacy Impact Assessments where possible
- Implement a Data Protection Officer
- Understand CCTV usage



What do schools need to do?

“The new regulation requires each school to complete an Information Asset Register (IAR).”

Letter from EA - 27 April 2018

- <http://www.eani.org.uk/about-us/think-data/>

Information Asset Register



Information Asset Register for schools - Final-4-2 — Saved to my Mac

Home Insert Page Layout Formulas Data Review View

Public task

	A	B	C	D	E
1	GDPR support for School Information Assets: Data Audit/Log				
2	Please read important notes and comments				
3					
4					
5		Last updated:			
6	Data Protection Officer (DPO):	By:			
7	Data Controller:				
8	Data Processor:				
9					
10	Data held or collected by the school	Data label *	Information Asset Owner	Who has role / access to enter information	Where is the data kept?
11	Information assets		<i>(Add your named person)</i>	<i>Enter specific names for dedicated role holders</i>	<i>Enter as appropriate (below are examples ONLY)</i>
12	Pupil data (within MIS)				
13	Pupil records	Special Categories of Personal Data*		SAO/office administrators	In MIS system
14	Welfare / Safeguarding / Child Protection data	Special Categories of Personal Data*		Head / named child protection officer	In a locked filing cabinet in a secure room
15	SEN	Special Categories of Personal Data*		SENCO/SAO / class teachers / Deputy	In a locked filing cabinet in a non-secure room
16	EAL	Special Categories of Personal Data*		EAL Lead / administrator	Staff laptop
17	Exclusion, behaviour	Special Categories of Personal Data*		Class teacher / Pastoral tutor / Headteacher	School network drive
18	Reports	Special Categories of Personal Data*		Class teacher / Pastoral tutor / Headteacher	Cloud storage
19	Examination results / Statutory Assessments	Special Categories of Personal Data*		Teachers / Exams Officer/Head of Dept.	Encrypted, password protected USB drive
20	Exams bodies exports	Personal* Data		Teachers / Exams Officer/Head of Dept.	In MIS system
21	Exams exports for Fisher Family Trust System (FFT)	Personal* Data		Teachers / Exams Officer/Head of Dept.	In MIS system
22	Attendance registers	Personal* Data		Class teachers / office administrators	
23	Student photos	Special Categories of Personal Data*		SAO/office administrators / class teachers	
24	Pupil Admissions	Special Categories of Personal Data*		SAO/office administrators	In MIS system
25	Other Admission data	Personal* Data			
26	Staff data (within MIS)				
27	Staff Personnel File	Special Categories of Personal Data*		SAO/office administrators	
28	Performance / CPD data	Personal* Data		SAO/Bursar / Deputy	
29	Staff absence data	Special Categories of Personal Data*		SAO/ Deputy	
30	Staff photos	Special Categories of Personal Data*		SAO/office administrators	
31	Employment Data	Special Categories of Personal Data*		SAO/office administrators	
32	Other Personnel Data				
33	Recruitment records for new headteacher	Special Categories of Personal Data*		SAO / Recruitment Panel	
34	Recruitment of new staff	Special Categories of Personal Data*		SAO / Recruitment Panel	
35	DBS / vetting checks	Special Categories of Personal Data*		Head / SAO	
36	Appraisal / CPD data	Special Categories of Personal Data*		SAO/Bursar / Deputy	
37	Disciplinary and grievance records	Special Categories of Personal Data*		Head / SLT / Panel	
38	Allegation of a child protection matter	Special Categories of Personal Data*		Head / Panel	
39	Malicious allegation of a child protection matter	Special Categories of Personal Data*		Head / Panel	
40	Health and safety assessments	Public data		H&S lead / teachers	
41	Health and safety accident reports	Special Categories of Personal Data*		H&S lead / Head / site manager	

Information asset owners Notes - important to read

http://www.eani.org.uk/_resources/assets/attachment/full/0/77232.xlsx



Some useful links

- <https://ico.org.uk/for-organisations/education/education-gdpr-faqs/>
- <https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>
- <https://ico.org.uk/for-organisations/data-protection-reform/getting-ready-for-the-gdpr/>
- <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notice-transparency-and-control/>
- <http://www.eani.org.uk/about-us/think-data/>

Data – in general



Visitors to the website	Staff (current/potential/substitute)	Suppliers	Children	Fundraising/Marketing

Data – the details



Data	Source of data	What do we do with this data	Lawful Basis	Action to be taken	Data limitation	Where stored?



Thank you, questions and
feedback

<https://vsitd.co/NAHTPART2>