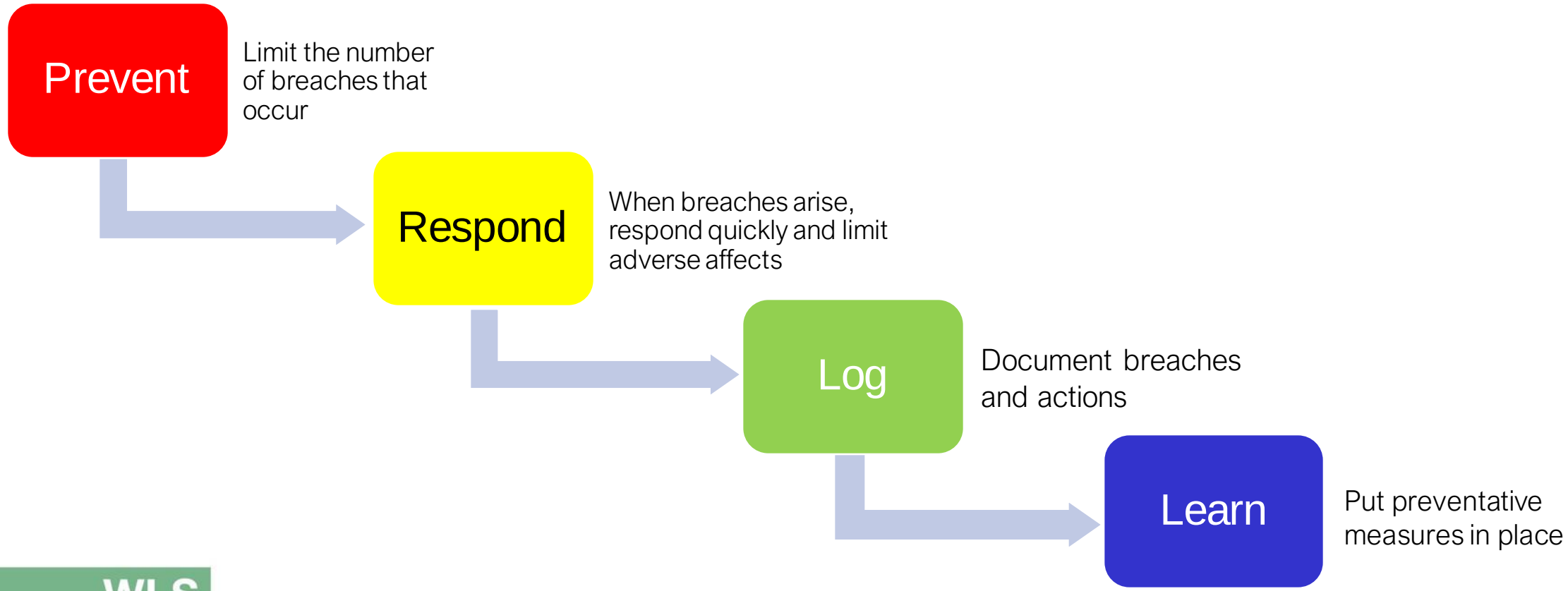
Handling Data Breaches

DPO Service

April 2021

WLS
Warwickshire Legal Services

What do we need to do?



Prevent Breaches from Happening in the First Place

SCHOOL DATA PROTECTION OFFICER

- You should have measures in place to protect the information you are holding.
- Effective measures will minimise occurrences of breaches
- Information Security Policy.
- We will cover this more in detail at the **Information Security** webinar (Tuesday 6th July, 11am)

Information must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

- Article 5

WLS
Warwickshire Legal Services

Report Data Breaches

- Notify the ICO of reportable breaches within 72 hours of discovery.
- Before you do so, you need to have the following information available:
  - Personal data that has been breached.
  - Number of data subjects.
  - Name and contact details of the DPO and DPL.
  - The likely consequences of the breach.
  - Measures taken or proposed to address and mitigate the effects of the breach.

"The controller shall….not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

- Article 33

WLS
Warwickshire Legal Services

Keep a Record of Breaches

SCHOOL DATA PROTECTION OFFICER

- Log all breaches (and near misses!)
- There needs to be enough detail to show what happened and how the breach was handled. Record:
  - Facts of the breach
  - The possible adverse effects
  - Remedial action taken

"The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Commissioner to verify compliance."

- Article 33

WLS
Warwickshire Legal Services

Remember, the purpose of your breach log is not only to demonstrate compliance, but also to ensure that you have sufficient notes on breaches, should you need to refer to the information again.

		DETAILS OF THE BREACH						CONSEQUENCES OF BREACH	MEASURES TAKEN/ TO BE TAKEN?			
NO.	REF.	Date/time of incident	No. of people whose data is affected	Nature of breach	Description of how breach occurred	How did you become aware of the breach/When was breach reported to you?	Description of personal data involved		What remedial action was taken?	Have the affected data subjects been informed?	Has the DPO been informed?	Does the breach need to be reported to the ICO?
1	01	01/03/2018	1	Email sent to wrong person.	Human error.	Parent emailed us.	Name and school work.	Others will know information.	Mum has deleted email.	Yes	Yes	No
2	02	01/03/2018 1:30pm	1	A pupil's school report was sent to the wrong parent. AC's report was sent to BC's parents. Both are in class 1M.	Office manager sent emails and accidentally confused the parents due to them having the same surname.	BC's Mum sent the school an email at 5:20pm. She stated that she didn't think the report was for her so has deleted the email.	Child's name, details of progress in work subjects.	Low level risk – BC's Mum has confirmed that she did not read the report and has deleted it. Had the report been read, it is unlikely that the pupil or family would suffer adversely as there was no embarrassing or sensitive information. The information has also only been disclosed to 1 individual and has been contained.	Staff have been reminded to double check the recipient's email address before sending out the reports. We will also disabled the auto-complete function when completing long tasks like this.	Yes. DPO confirmed it is not a requirement as risks are low level. However, there is a possibility that BC's mum could mention it to AC's parents so we have called them to apologise.	Yes – incident form completed and forwarded at 9:30am on 2 March. Followed recommendations to ensure breach is contained, logged and steps put in place to reduce risk of reoccurrence.	No

Could another person read it and understand what happened?

Processors

- If one of your processors suffers a data breach they must inform you without due delay.
- The school, as data controller, are **responsible for assessing and reporting the breach** (if required).
- It does not matter that the school may not be responsible for the breach.
  - The school will be best placed to make assessment because of their knowledge of the data subjects.

> *"The processor shall notify the controller without undue delay after becoming aware of a personal data breach."*
> - Article 33

WLS
Warwickshire Legal Services

How do we risk assess breaches?

1. What are the **risks**?
2. Is it **likely** that the risks will occur?
3. How **severe** are the consequences?
4. Are there any **mitigating** factors?

You need to think about these *before* you report to the DPO or ICO.

The DPO Service will assist wherever possible. However, you will know the context and factors for consideration.

WLS
Warwickshire Legal Services

1. Risks

Type of Risk	Example
Loss of Control	A photo of a vulnerable child is accidentally shared on the school's social media. The post is taken down a few days later. The school don't know who has seen or copied the information.
Discrimination	Information about a person's sexual orientation or belief is inadvertently disclosed. The individual experiences bullying as a result of the breach.
Embarrassment	A pupil's grades are sent to the wrong pupil. The pupil's scores are at the lower end of possible scores.
Identify Theft or Fraud	ID and bank account details are accessed through a ransomware attack.
Damage to Reputation	Notes relating to a disciplinary meeting are sent to the wrong member of staff.
Loss of Confidentiality	Private data relating to an individual's health condition are disclosed to others.
Lack of Availability	A school has only one paper copy of an important document which is accidentally shredded.

This is not an exhaustive list!

2. Likelihood

Likelihood	Example
Remote	An email about a pupil is sent to a teacher who works in a different school. The schools are part of the same academy trust. The teacher who receives the email realises it has been sent in error and deletes it from *Inbox* and *Deleted* folder before reading it.
Unlikely	A generic email containing no personal data is sent out to 31 parents. The sender forgets to use Bcc. The sender quickly asks all parents to delete the email and confirm when they have done so. The school assesses the risks by checking whether any parents may be at risk as a result of their email address being breached. There are no concerns raised in their investigations.
Likely	Information about a child, including their address, is sent by tracked post but lost by the courier. The school investigates but the courier cannot place the whereabouts of the package.
Very Likely	A child has a medical condition which is private and not known to other pupils. Information about the condition is contained in a document on the school's OneDrive. Errors with access settings mean that the whole class can now view the information. The school finds that most children have accessed the document.

These are examples only – always assess each incident on a case-by-case basis.

3. Severity

Consider the impact that the breach will have on the individual/individuals.

Severity	Example
Low	There is a connection failure which prevents the school from sending out a newsletter with general updates. The school send it out the following day.
Medium	A copy of a class list is found lying around in the playground.
High	Information relating to the truancy and behaviour of a group of 30 pupils is accidentally sent to the parents of all pupils in the school.
Very High	An individual moves house to hide their location from another person. The individual's new address is disclosed in error to the other person. This jeopardises the safety of that individual.

This will case specific.

4. Mitigating Factors

Some factors may limit the likelihood or severity of a breach occurring:

Mitigating Factor	Example
Information is already public	A child's information, disclosed in error, states that the child has asthma. As this is medical data, it is classed as *special category data*. However, this information is fairly well known among classmates and teachers. Therefore, the breach is unlikely to pose many risks to the child.
Employees of the same organisation	Sensitive information about a pupil is sent to a member of staff who works in the same school, but would not have normally had access to this information. **N.B. Info about other employees could be damaging.**
Disclosure to one person	An email is erroneously sent to a group of 60 parents in error. The school realises straight away and recalls the email from all except on recipient.
Intention of Recipient	Data appropriated with the intention of causing harm vs data disclosed to an individual, in error, who is known to the school and deemed trustworthy.

WLS
Warwickshire Legal Services

When to report to the ICO?

Considering:

- Risks
- Likelihood
- Severity
- Mitigation

Yes = report to ICO

No = follow up yourself

Is it **likely** that the data subject(s) will be put at risk as the result of the breach?

'When a personal data breach has occurred, you need to establish the likelihood of the risk to people's rights and freedoms. ***If a risk is likely, you must notify the ICO; if a risk is unlikely, you don't have to report it.*** *However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.'*

- ICO

WLS
Warwickshire Legal Services

When to inform the data subjects?

Considering:

- Risks
- Likelihood
- Severity
- Mitigation

Yes = report to ICO

No = follow up yourself

You can exercise your discretion

Is it **highly likely** that the data subject(s) will be put at risk as the result of the breach?

N.B. The threshold for informing data subjects is *higher* than for reporting it to the ICO.

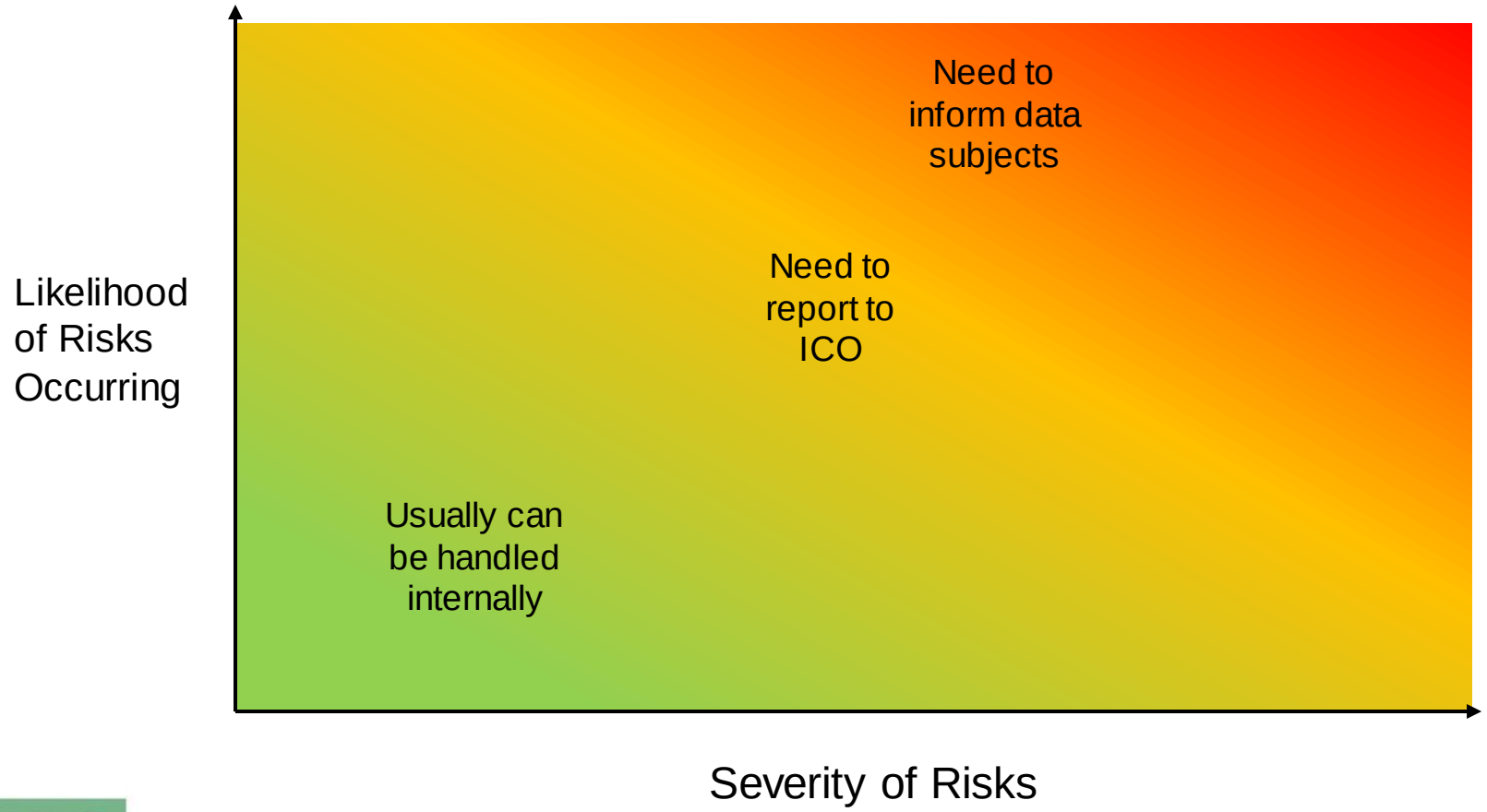
This allows individuals to protect themselves.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR says you must inform those concerned directly and without undue delay.

- ICO

WLS
Warwickshire Legal Services

Informing the ICO and Data Subjects



WLS
Warwickshire Legal Services

How do we prevent breaches?

- Systems Security
- Policies and Processes
- Training
- DPIAs where required

Systems Security

- This requires specialist knowledge – consult your IT provider
- The majority of personal data is in electronic form
- Encryption
- Strong passwords
- Checking access controls
- Are home working arrangements secure?
- Deleting information in line with your retention schedule

SCHOOL DATA PROTECTION OFFICER

WLS
Warwickshire Legal Services

Policies and Processes

- Data Protection Policy
- Information Security Policy
- Written data breach procedure (see Appendix to DPP)

Appendix 1: Personal data breach procedures

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, the [School / Academy Trust] will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.

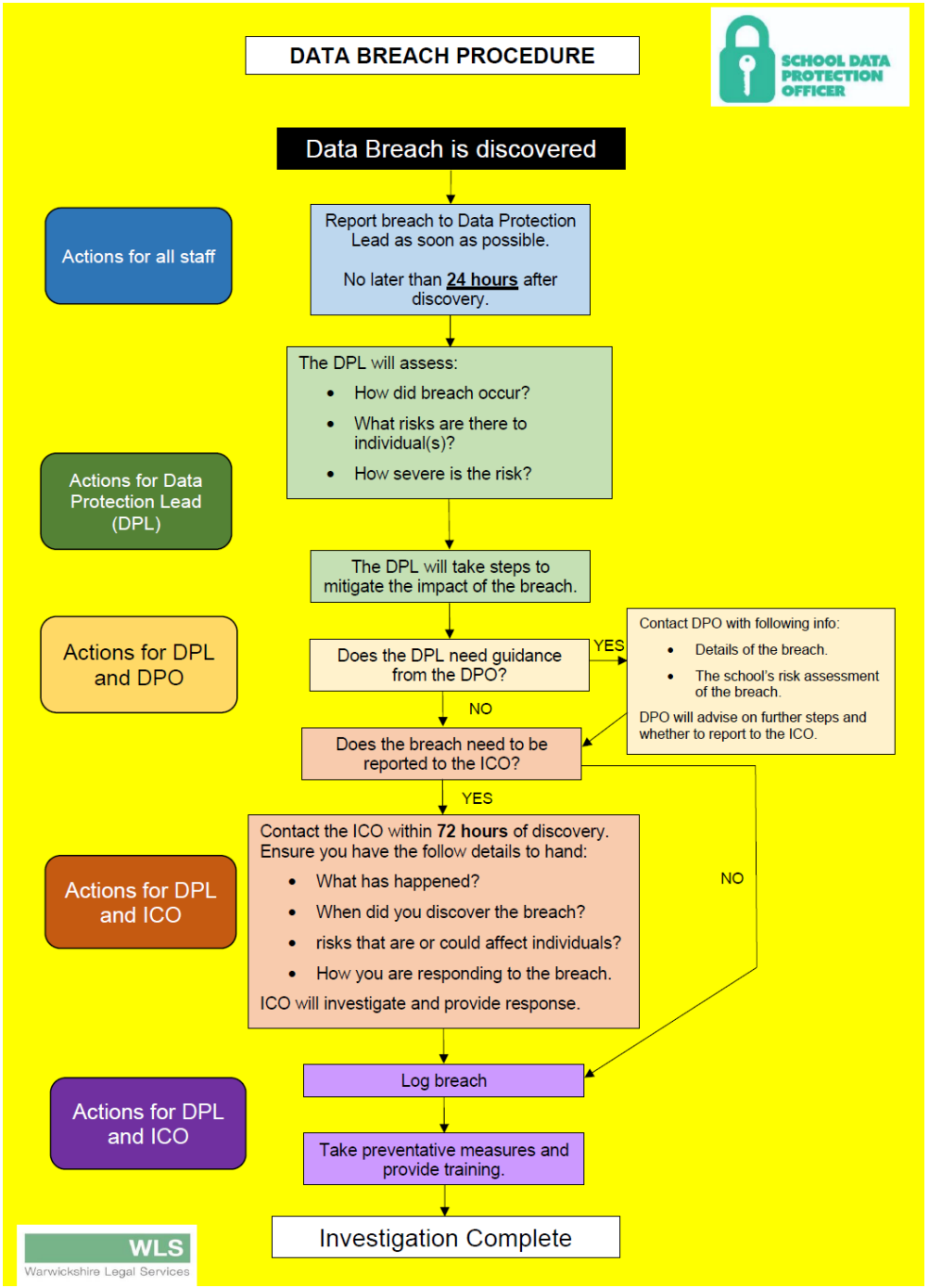
2. Examples of how a breach may occur include:

    a. Theft of data or equipment on which data is stored;
    b. Loss of data or equipment on which data is stored;
    c. Inappropriate access controls allowing unauthorised use;
    d. Accidental Loss;
    e. Destruction of personal data;
    f. Damage to personal data;
    g. Equipment failure;
    h. Unlawful disclosure of personal data to a third party;
    i. Human error;
    j. Unforeseen circumstances such as fire or flood;
    k. Hacking attack; or
    l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.

3. If any member of staff of the [School / Academy Trust], or [Governor / Trustee], discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to notice, inform the [School / Academy Trust]'s Data Protection [Champion / Contact].

4. Upon being notified, the [School / Academy Trust]'s Data Protection [Champion / Contact] will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the [School / Academy Trust]), then the [School / Academy Trust]'s Data Protection [Champion / Contact] will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.

Do staff know your procedure?



WLS
Warwickshire Legal Services

Training

- All schools should be providing annual refresher training.
- The key issues of both policies should be included in training sessions.
- Regular feedback and reminders to reduce likelihood of human error.
- If similar breaches recur, consider whether further action is needed.

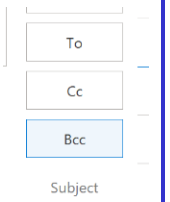
DPIAs

- High risk, novel or complex data processing requires a DPIA.
- This will enable you to identify risks in advance.
- If you implement a new system, and do not need to complete DPIA, you should still consider potential risks before full implementation.

Common Breaches

1. Emailing numerous individuals without using ***Bcc***.
2. Using images without consent.
3. Forgetting to redact information.
4. Sending information to the wrong individual.
5. Leaving personal details on a voicemail.
6. Losing paper notes and files.

1. Make sure your email settings automatically show Bcc.



2. Ensure all staff have lists of children who have consent for photographs.
3. Consider audience. Second pair of eyes.
4. Disable auto-complete. Double check recipient (especially when sending out numerous emails).
5. Avoid leaving personal information on a voicemail.
6. Lock paper files away. Observe clear desk policy.

WLS
Warwickshire Legal Services

Any Questions?

Next webinars:

Subject Access Requests	Tuesday 8th June, 11am
Information Security	Tuesday 6th July, 11am