07.05 Data breach policy

Information about children and their families (data subjects) is recorded and shared in line with the eight principles of the General Data Protection Regulations (GDPR) (2018).
The eight principles state that personal data must be:

1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept for longer than is necessary
6. Personal information must be processed in line with the data subject's rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection (in circumstances where this may happen e.g. Facebook additional permission is sought from the parent)

The GDPR and Essex County Council places obligations on staff to report actual or suspected data breaches and the procedure for dealing with breaches is set out below. Training is provided to all staff to enable them to carry out their obligations within this policy.

Data breach procedure

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental, deliberate or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or sensitive/special category data transmitted, stored or otherwise processed.

Examples of a data breach could include, for example:

- accidental or deliberate loss or theft of data or equipment on which data is stored, for example loss of a laptop, memory stick or a paper file
- unauthorised access to data by a third party
- equipment failure
- sending data to the incorrect recipient
- alteration of personal data without permission
- unforeseen circumstances such as a fire or flood
- hacking of a laptop
- encrypted by ransomware

Reporting a data breach

If you know or suspect a personal data breach has occurred, you should discuss the breach with the manager Pam Biddulph (Data Protection Officer - DPO) and complete a Data Breach Report form if appropriate. If necessary, further guidance will be sought from Jenny Walker (trustee and additional Data Protection Officer).

Staff are expected to seek advice from the manager if they are unsure as to whether the breach should be reported.

Once reported to the DPO, staff should not take any further action in relation to the breach. In particular staff must not notify any affected individuals or regulators or investigate further.

Managing and recording the breach

On being notified of a suspected personal data breach, Pam Biddulph (DPO) will take immediate steps to establish whether a personal data breach has in fact occurred and will consider whether this poses a risk to the people involved. The DPO will need to consider the likelihood and severity of the risk to people's rights and freedoms following the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the DPO must inform those individuals immediately.

Steps will be taken to:

- where possible, contain the data breach
- as far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed
- assess and record the breach in the pre-school's data breach register
- notify the ICO if necessary
- notify Essex County Council Information Governance Team and Procurement Team, if necessary, by:
    - in the first instance, emailing ECC on the following email addresses, without enclosing any personal data or commercially sensitive information, to notify them of the breach:
        - informationgovernanceteam@essex.gov.uk
        - commercial.team@essex.gov.uk
    - ECC will respond via secure email for further detail as required
    - ECC must be kept updated on the investigation progress and final resolution as directed
- notify data subjects affected by the breach
- notify other appropriate parties to the breach
- notify insurers, police for example, if the breach involved theft of equipment or data
- take steps to prevent future breaches

This is not an exhaustive list.

Notifying the ICO

DPO's Pam Biddulph and/or Jenny Walker will decide if the ICO needs to be notified.

Guidance from the ICO website:

If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of the risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report. You do not need to report every breach to the ICO.

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.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

How much time do we have to report a breach?

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

What if we don't have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate

it. So Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, we expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify us of the breach when you become aware of it, and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to us and tell us when you expect to submit more information.

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see go to www.ico.org.uk/for-organisations/report-a-breach

Notifying data subjects about a breach

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says the DPO must inform those concerned directly and without undue delay and so this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. The DPO will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again, the risk is higher. In such cases, the DPO will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If the DPO decides not to notify individuals, they will still need to notify the ICO unless they can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The DPO should also remember that the ICO has the power to compel them to inform affected individuals if the ICO considers there is a high risk. The DPO will document their decision-making process in line with the requirements of the accountability principle.

Information provided to data subjects when telling them about a breach

The DPO will describe the nature of the personal data breach and will give:

- their name and contact details or another contact point where more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Other steps required by GDPR to take in response to a breach

Records of all data breaches will be recorded, regardless of whether or not they were reported to the ICO.

Article 33(5) requires the DPO to document the facts relating to the breach, its effects and the remedial action taken. This is part of the pre-school's overall obligation to comply with the accountability principle, and allows the ICO to verify our organisation's compliance with its notification duties under the GDPR.

Assessing the breach and preventing further data breaches

Once the initial reporting procedures have been carried out, the pre-school DPO will undertake an investigation into how the breach occurred and will take immediate action to stop or reduce further loss or unauthorised disclosure of personal data. Where possible the pre-school will try to recover lost data.

The pre-school will then undertake a risk assessment as to what further steps need to be taken to ensure a recurrence of the data breach can be prevented.

All staff are encouraged to make Pam Biddulph (DPO) aware of any data handling concerns that they may come across in the pre-school so that they can be rectified and avoid any data breaches.

Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

Guidance from ICO website

What else should we take into account?

The following aren't specific GDPR requirements, but you may need to take them into account when you've experienced a breach.

It is important to be aware that you may have additional notification obligations under other laws if you experience a personal data breach. For example:

- *If you are a communications service provider, you must notify the ICO of any personal data breach within 24 hours under the Privacy and Electronic Communications Regulations (PECR). You should use our PECR breach notification form, rather than the GDPR process. Please see our pages on PECR for more details.*
- *If you are a UK trust service provider, you must notify the ICO of a security breach, which may include a personal data breach, within 24 hours under the Electronic Identification and Trust Services (eIDAS) Regulation. Where this includes a personal data breach you can use our eIDAS breach notification form or the GDPR breach-reporting process. However, if you report it to us under the GDPR, this still must be done within 24 hours. Please read our Guide to eIDAS for more information.*
- *If your organisation is an operator of essential services or a digital service provider, you will have incident-reporting obligations under the NIS Directive. These are separate from personal data breach notification under the GDPR. If you suffer an incident that's also a personal data breach, you will still need to report it to the ICO separately, and you should use the GDPR process for doing so.*

You may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

The EDPR, which has replaced WP29, may issue guidelines, recommendations and best practice advice that may include further guidance on personal data breaches. You should look out for any such future guidance. Likewise, you should be aware of any

recommendations issued under relevant codes of conduct or sector-specific requirements that your organisation may be subject to.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.