DIOCESE OF CHICHESTER
ACADEMY TRUST

Data Breach Policy

June 2021

DIOCESE OF CHICHESTER ACADEMY TRUST

DATA BREACH POLICY

Date Agreed:	**June 2021**
Review Date:	**June 2023**
Type of Policy:	**DCAT Statutory Policy**

Revision Number	Date Issued	Prepared by	Approved	Personalised by school	Comments
3	April 2021	DCAT	Trust Board		
2	June 2020	CF			DPO
1	24th May 2018	SJP/DC	DCAT		JUDICIUM

Type of Policy	*Tick* ✓
DCAT Statutory Policy	
DCAT Non-statutory Policy	✓
DCAT Model Optional Policy	
Academy Policy	
Local Authority Policy	

Contents

Introduction

Our **vision** for our Trust is we exist to:

Help every child achieve their God-given potential

Our **aims** are clear. We aim to be a Trust in which:

Developing the whole child means pupils achieve and maximise their potential

Continued development of staff is valued and improves education for young people

All schools are improving and perform above national expectations

The distinct Christian identity of each academy develops and is celebrated

Our work as a Trust is underpinned by shared **values**. They are taken from the Church of England's vision for Education and guide the work of Trust Centre team. They are:

Aspiration
I can do all things through Christ who strengthens me
(Philippians 4 vs 13).

Wisdom
Listen to advice and accept discipline, and at the end you will be counted among the wise
(Proverbs 19 vs 20)

Respect
So in everything do to others what you would have them do to you
(Matthew 7 vs 12)

Our vision of helping every child achieve their God-given potential is aligned with the Church of England's vision for education and is underpinned by the Bible verse from John: *I have come that they may have life, and have it to the full.*

1. Policy Aims

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data. Personal data is defined as any information relating to an identified or identifiable natural person. The person is known as the 'data subject'.

The sixth principle of data protection states that personal data shall 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'.

Notwithstanding the measures that Data Controllers put in place, it is inevitable that sometimes a failure will occur with respect to this principle, creating a personal data breach. Three types of breaches are recognised:

- Confidentiality – unauthorised access or use of personal data
- Availability – Personal data that should be available is not accessible
- Integrity – Inaccurate personal data has been recorded

The GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the Trust of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. 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.

In the event of a data breach, there are a set of key actions which must be undertaken.

The Trust is the registered Data Controller, however, most information will be stored at School level and therefore the terms "Trust" and "School" should be interchangeable throughout this policy.

2. Definitions

2.1 Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can

reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

2.2 Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

2.3 Personal Data Breach

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

2.4 Data Subject

Person to whom the personal data relates.

2.5 ICO

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

3. Responsibility

The DPO has overall responsibility for breach notification within the Trust. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of the DPO, please do contact the Head of Operations & Governance.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines. The DPO will:

- Provide guidance and support to the School/Trust in dealing with a personal data breach
- Provide a route of communication to the Information Commissioners Office (ICO) in the event of notification being required and any follow up action

Please contact the DPO with any questions about the operation of this policy or the GDPR Lead at your School if you have any concerns that this policy is not being or has not been followed.

The School will:

- Nominate a staff member responsible for GDPR within the School who will be the School GDPR Lead
- Follow the clear procedure for dealing with personal data breaches.
- Follow any additional guidance from the Information Commissioners Office (ICO) produced subsequently to this policy
- Inform the Trust DPO of all personal data breaches
- Record the details of personal data breaches and make those records available to the Trust DPO
- Ensure that personal data breaches are dealt with in line with the statutory time limits and notify the DPO as soon as possible if these limits can't be met
- Take advice from the DPO with regards to the management of personal data breaches

The DPO's contact details are set out below: -

Data Protection Officer: Claire Friend
Address: DCAT, St Catherine's College, Priory Road, Eastboune BN23 7BL
Email: dpo@dcat.academy
Telephone: 01273 056292

4. Security and Data-Related Policies

Staff should refer to the following policies that are related to this data protection policy: -

Security Policy which sets out the Trust's guidelines and processes on keeping personal data secure against loss and misuse.

Data Protection Policy which sets out the Trust's obligations under GDPR about how they process personal data.

These policies are also designed to protect personal data and can be found here

5. Data Breach Procedure

3.1 What Is a Personal Data Breach?

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

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

3.2 When Does It Need to Be Reported?

The School/Trust must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

3.3. Procedure Overview

The procedure for managing personal data breaches needs to be implemented in detail by the GDPR Lead within the School and in liaison with the Trust DPO.

- Discovery & reporting of a personal data breach
- Investigate the nature of the breach
- Action to contain the breach
- Assess the level of notification required
- Notify appropriate parties
- Identify actions to minimise the recurrence of the breach

6. Discovering & Reporting a Data Breach

This section covers both the initial recognition that a breach has occurred and the notification to the GDPR Lead within the School and the Trust DPO to enable action to be taken.

Any member of staff at the Trust/School may identify that a breach has potentially occurred. They may also receive a report from a student or any other stakeholder that a potential breach has occurred.

Reporting a breach makes a positive contribution to the Trust/School managing its data protection responsibilities.

Although not all personal data breaches are reported to the Information Commissioners Office (ICO), each incident should be treated as though it might be until the evidence shows otherwise.

In the case of a personal breach that must be reported to the ICO, there is a 72-hour window. It should be noted that at the point any member of staff becomes aware of a potential breach that this is the start of the 72-hour window, not when the DPO is informed.

Members of staff are not expected to independently investigate potential breaches before bringing them to the attention of the DPO as this will reduce the time available for the GDPR Lead within the School and the DPO to manage the issue.

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- Complete a data breach reporting form
- Email the completed form to dpo@dcat.academy

The Trust has provided the DPO email address for communications about data protection issues. Each School must have a GDPR lead and we need to ensure that there are communication routes (telephone and email) for contact outside of normal working hours or outside of term times.

Where appropriate, you should liaise with your line manager about completion of the data breach report form. Breach reporting is encouraged throughout the School/Trust and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators or investigate further. The DPO will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report.

7. Managing, Recording & Containment of the Breach

From the initial report, it is essential to establish a chronology for the breach. This will later include information about actions taken and impact assessments. At this first stage the person reporting the breach needs to provide:

- The time and date that the suspected breach was detected
- A description of the nature of the breach including classification (Confidentiality, Availability, Integrity)
- The data subjects, types of personal data and number of records affected
- How the individual identified the potential breach
- Details of any individuals they have discussed the potential breach with.

If there are emails or other notes, call records or any other materials associated with the discovery of the breach, these should be provided although it is recognised that there may be a delay in assembling all the material.

It should be noted that depending on the exact circumstances, the person who has identified the potential breach may have minimal information.

On being notified of a suspected personal data breach, the Head Teacher or the GDPR lead within the School, will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps 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 School's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

Containment means taking action that mitigates the potential consequences of the breach. Providing a breach has been reported quickly, significant mitigation may be possible. In some cases, especially with confidentiality breaches, the time gap between the initial breach and its discovery leaves little room for containment.

Before undertaking any action, an assessment must be made to ensure that it doesn't compound the breach – for example by disclosing personal data to unauthorised recipients.

If, at this point, criminal activity is suspected (even tangentially, such as the theft of a car containing personal data), the police should be informed, and the crime number should be recorded. If there is strong evidence that a member of the School/Trust community has deliberately breached information, then appropriate disciplinary action needs to be initiated.

Even if the actual breach event happened some time before discovery, the questions about whether actions can be taken to mitigate the further spread of breached information should be considered. It can of course be far more difficult to achieve in these circumstances.

Whatever decisions and actions are taken, should be recorded in the breach log chronology.

7.1 Notifying the ICO

The DPO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If the Trust/School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

7.2 Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Head Teacher or Business Manager will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the School/Trust have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the Head Teacher or the Business Manager will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School/Trust will consider alternative means to make those affected aware (for example by making a statement on the School/Trust website).

7.3 Notifying Other Authorities

The School/Trust will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

8. Investigating & Assessing the Breach

The core focus at this stage is to have enough information to determine if notification to the ICO will be required. The report from the individual who discovers the breach may not have sufficient detail to make the decision. To make this decision the essential information is:

This is a decision that must involve the Trust DPO.

Once initial reporting procedures have been carried out, the School/Trust will carry out all necessary investigations into the breach.

The School/Trust will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School/Trust will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the School/Trust; and
- Any other wider consequences which may be applicable.

Highly confidential information about a small number of people could have very significant impact on them or other people, while relatively benign data about many people may have little risk to their rights and freedoms.

Each case must be decided upon it's specific circumstances. The GDPR lead at the School must be aware that the Trust DPO, in fulfilling their role, may decide that the ICO must be alerted even though the GDPR Lead has decided not to report an incident. The rational for the decision about

reporting should be recorded and kept with other details of the breach. If a judgement is made that the ICO must be notified, then it is likely that further investigation will be required before the report can be completed. This means that the decision about notification really needs to come before the 72-hour window closes.

9. Preventing Future Breaches

Once the data breach has been dealt with, the School/Trust will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it's necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

For organisations to be fully GDPR compliant they need to be able to demonstrate that they have engineered data protection by default and by design into their operations. One element of that is to look for continuous improvement in the data protection regime.

Any incident that has been recorded on the breach log should be subject to review. This will be undertaken by the Trust DPO and the Head of Operations & Governance along with the GDPR Lead at the School and the Head Teacher.

It may be that the review of an individual case identifies weaknesses in the data protection regime and consideration needs to be given as to how these weaknesses can be addressed. It may be that during the process of review, a pattern of incidents is identified. These patterns may reveal something systematic in the organisation that needs to be addressed.

The DPO can consider whether a Data Protection Impact Assessment (DPIA) would be useful to identify specific weaknesses in the processing of personal data in the area of the breach.

10. Possible Indications of personal data breaches

The items described in this section form a very small subset of the signs that a breach has occurred. It is essential to remember that there is no requirement to know that the rights and freedoms of individuals have been infringed to recognise that a breach has occurred. It is enough that the infringement could happen. Consider the three types of personal data breaches – confidentiality, availability and integrity.

10.1 Confidentiality Breaches

Here we are concerned about information falling into the hands of people unauthorised to have it. Obvious cases would be:

- Loss or theft of a computer, tablet or phone containing, or with access to, personal data
- Loss or theft of a personal bag containing paper records of personal data
- An individual having access to, or a copy of, personal data not required for their role
- Sending an email to the wrong location
- Disclosing the identity of recipients of an email when those recipients might otherwise reasonably expect confidentiality
- Passing on information about a data subject from an individual who is entitled to know to one who is not entitled

In some cases, it would be relatively easy to identify that the breach had occurred, but in others the initial indications of the breach maybe quite diffuse.

In extreme cases, the first indication of a breach is the lodging of a complaint to the School/Trust or the appearance of stories in the traditional media or in social media spaces.

10.2 Availability Breaches

An availability breach is probably the easiest to spot because information is not available when it's required. Possible causes might be:

- A failure of a system like the Management Information System (MIS) HR Database or Visitor Management
- A file not being returned to its storage location
- A file being shredded before the end of its retention period
- Records being erased before their retention period
- Theft, fire or vandalism

There are thresholds to consider in the case of an availability breach. If a system is down for a short period of time, or missing for a short period, then this would almost certainly not meet the threshold. The question is whether the lack of availability could have an impact on the rights and freedoms of the data subjects that the information related to.

10.3 Integrity Breaches

Integrity Breaches occur when personal data is inaccurate. There are two major ways that this occurs.

- Data is captured inaccurately
- The data becomes out of date

The breach only appears at the time the data is being retrieved or used and the potential impact of the breach can be highly variable.

11. Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the DPO. This can help capture risks as they emerge, protect the Trust/School from data breaches and keep our processes up to date and effective.

12. Related Policies

Staff should refer to the following policies that are related to this Data Breach Policy

- Data Breach Policy
- Data Retention Policy
- CCTV Policy
- Information Security Policy
- Freedom of Information Policy
- Privacy Notices
- Electronic Systems and Information Policy.