From:	information.compliance@powys.gov.uk
To:	icocasework@ico.org.uk;
CC:	
Subject:	Personal Data Breach Notification
Direction:	Incoming
Date Received:	17/03/2023 16:26

External: This email originated outside the ICO.
Please find attached a personal data breach notification made on behalf of St Michaels Church in Wales Primary School. If you have any further questions then please do not hesitate to be in contact.

Regards

3rd party PD
3rd party PD
Digital Services - Gwasanaethau Digidol
Cyngor Sir Powys County Council
3rd party PD

Croeso i chi gysylltu â ni yn Gymraeg. Byddwn yn ymateb yn Gymraeg, heb oedi. / You are welcome to contact us in Welsh. We will respond in Welsh, without delay.

Llun yn cynnwys eiconau tai, ceir a bryniau. Picture including icons of houses, cars and hills.

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. **Please do not include any of the personal data involved in the breach when completing this form**. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- (•) Initial report
- ( ) Follow-up report

(Follow-up reports only) ICO case reference:

Reason for report – after consulting the guidance

- ( ) I consider the incident meets the threshold to report
- (•) I do not consider the incident meets the threshold to report, however I want you to be aware
- ( ) I am unclear whether the incident meets the threshold to report

About the breach

Please describe what happened

Parents refused consent for their child's image to be taken or placed on any digital platform. They had initially refused consent for any photo to be taken. However, the School explained that they have a lawful basis for taking photo's and video's in order to evidence achievement for a reception age child (Article 6 (1)(e). Estyn (School Inspectorate in Wales), during School Inspections, want to see evidence of a child's academic progression and photographic/video evidence for young children, who don't do much, if any , written work is

deemed by professionals and Estyn to be a good way of evidencing attainment in the curriculum.
See link for more information School improvement guidance: framework for evaluation, improvement and accountability - Hwb (gov.wales).

The School agreed with the parents request in regard to not placing images on any other platform including Hwb - a Welsh Government platform for storing of information, lesson plans, evidence and resources, as the evidence could be provided by photos printed from digital cameras & ipads and placed in the child's work book.

However, the School was alerted by the parent that they could view their child on a video through the Hwb platform. The School identified the video, which contained images not just of the complainants child but other children in the same class, participating in academic activites. An investiagtion followed which quickly identified human error and the video was removed completely.

A complaint was raised by the parents that they could still view the video and that the school were not taking the matter seriously. School confirmed with Hwb that the offending video was removed. The School has been in communication with the parents via numerous emails and the parents were asked to provide the URL of the video that they claimed to be able to see in order that the School could trace back to source. These multiple requests have been ignored.

Please describe how the incident occurred

This happened because of human error - 3rd party PD uploaded class videos as evidence but failed to make the setting "private", it was set to public so allowing anyone to potentially view. There are multiple children on the video not just the child of the complainants. As soon as the School was alerted the setting was changed and then the video removed completely. As a belt and braces exercise the School has gone through all platforms and removed historic items and ensured that current videos have been set to private.

Children in reception classes do not have a Hwb log in as they are deemed too young so any evidence is uploaded to a class account maintained by the class teacher and learning support assistants. As there is no log in to share with the parent we are unsure as to how they have gained access to the video content.

Parents may have obtained access following a parents evening when QR codes containing links to pictures and video's used as part of the evidence trail were placed in children's work books. However, from recollection whilst the parent was offered the book to review they didn't do it.

How did the organisation discover the breach?

The School was alerted by the parents to the video's existence

What preventative measures did you have in place?

Staff have previously been reminded that all data including video content should be set as private.
Staff are aware that of the parents wishes that their child's image in not uploaded.

Was the breach caused by a cyber incident?

- ○ Yes
- ◉ No
- ○ Don't know

When did the breach happen?

Date: September 2022 Time:

When did you discover the breach?

Date: 09/02/23 Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☐ Basic personal identifiers, eg name, contact details
- ☐ Identification data, eg usernames, passwords
- ☐ Economic and financial data, eg credit card numbers, bank details
- ☐ Official documents, eg driving licences

☐ Location data, eg coordinates

☐ Genetic or biometric data

☐ Criminal convictions, offences

☒ Other (please give details below)

Image only

Number of personal data records concerned?

1

How many data subjects could be affected?

5

Categories of data subjects affected (tick all that apply)

☐ Employees

☐ Users

☐ Subscribers

☐ Students

☐ Customers or prospective customers

☐ Patients

☒ Children

☐ Vulnerable adults

☐ Other (please give details below)

Potential consequences of the breach

Parents are seeking legal advice. We have not been able to determine any detrimental effect to the child.

Is the personal data breach likely to result in a high risk to data subjects?

○ Yes

◉ No

○ Not yet known

Please give details

(Cyber incidents only) Recovery time

- ○ We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident
- ○ We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this
- ○ We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no current backup, backup encrypted etc
- ○ We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

Had the staff member involved in this breach received data protection training in the last two years?

- ◉ Yes
- ○ No
- ○ Don't know

(Initial reports only) If there has been a delay in reporting this breach, please explain why

There has been a delay in rpeorting because we did not consider that the breach met the threshold for reporting. However, given that the School has on multiple occasions asked the parents for the URL of the video that they maintain they can still see which has not been forthcoming and the fact that the parents are threatening legal action then we considered it prudent to self report so that the Regulator was aware of the issue.

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

The video was removed from the platform. All platforms have been checked to ensure that there is no further content involving the child. All platforms have been checked to ensure that settings are made private. Staff have been formally advised to take care when posting evidence on any platform.

Immediately after notification of the breach the Headteacher contacted Hwb to ask them whether they could find out how many times the content had been viewed but they were unable to advise, following this the Schools ICT Consultant (a purchased in advisor) has: reviewed the platform, has spoken with the Hwb platform to find out more about whether the images could still be viewed (after taking them off the site). He has also tried communicating with the parents to get a better understanding of where they can view the video and has asked them for the link to the video which has not been forthcoming. The School asked the parents to clear their cache incase it was stored there and their ability to continue to see the video was reliant upon that. The School have been advised by the parent that it was not in cached items. Finally the School have attempted to do a "Google images" search for any images in the public realm of the child. None have been found.

The School have sought advice on breach management from Powys County Councils Information Compliance Manager, have spoken to Welsh Government's digital leadership team and finally the Head Teachers union official to ensure that all avenues have been covered.

Have you taken actions to contain the breach? Please describe these remedial actions

Please see above.

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Staff have been reminded about personal data security and this will become a standing item on staff meeting agendas. Data Protection training has already been undertaken but will be reviewed again in the next few months for all staff. A checking regime for uploading to digital platforms will be introduced.

Have you told data subjects about the breach?

- ○ Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects
- ◉ Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway
- ○ No – but we are planning to because we have determined it is likely there is a high risk to data subjects
- ○ No – we determined the incident did not meet the threshold for communicating it to data subjects

Have you told, or are you planning to tell any other organisations about the breach?

- (•) Yes
- ( ) No
- ( ) Don't know

If you answered yes, please specify

Welsh Government Hwb Platform, Powys County Council for data protection breach management advice and guidance

About you

Organisation (data controller) name

St Michael's Church in Wales Primary School

Registration number

ZA243351

If not registered, please give exemption reason

Business sector

Education

Registered organisation address

St Michael's Church in Wales Primary School
Kerry
Newtown
SY16 4NU

Person making this report

In case we need to contact you about this report

Name: 3rd party PD

[redacted]

Email: information.compliance@powys.gov.uk

Phone: 3rd party PD

Data protection officer

Or the senior person responsible for data protection in your organisation

☐ Same details as above

Name: 3rd party PD

Email: 3rd party PD

Phone: 3rd party PD

Sending this form

Initial report
If this is your initial report, please send your completed form to icocasework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report
If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number. If we consider the incident is minor or you have indicated that you do not consider it meets the threshold for reporting, you may not receive a response from us.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.

From: icocasework@ico.org.uk
To: information.compliance@powys.gov.uk;
CC:
Subject: ICO Decision - IC-222646-S3Z0
Direction: Outgoing
Date Sent: 22/03/2023 09:13

Reference Number IC-222646-S3Z0

Dear 3rd party PD,

I am writing about the personal data breach report you submitted on 17 March 2023.

Thank you for the information provided.

Data security requirements

It is important to have appropriate technical and organisational measures in place to ensure the security of personal data.

Our decision

We have considered the information provided and we have decided not to take action. This decision is based on the information we have recorded about the breach.

Please note that we may make enquiries if we become aware of new information that affects the circumstances of this case.

We deal with thousands of personal data breach reports each year. In many cases, the breach could easily have been prevented. Please read our attached leaflet, which contains our tips for preventing the most common personal data breaches. If you're not doing these things already, please consider implementing them.

We also recommend you check that your policies and procedures are fit for purpose. All staff who handle personal data should receive regular data protection training. If you haven't already done so, you should implement any specific steps you identified to prevent a recurrence of this incident.

Thank you for reporting the breach. Further information and guidance relating to personal data breaches under the UK General Data Protection Regulation (UK GDPR) and data security is available on our website at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

We now consider the matter to be closed.

We're currently running an email survey to find out what customers think of our services and would like you to take part. The survey will take a few minutes to complete and will help us understand what we can do to improve our services in the future.

The Institute of Customer Service is running the survey on our behalf.

If you **don't** want them to email you our survey, please let us know by responding to this email by **5 April 2023** and we won't include you. There is information about the right to object to the use of your data on our website.

Yours sincerely

Caroline Browne
Lead Case Officer
0330 313 1724

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email

Personal data security: how to prevent some common personal data breaches in the Education sector

1. Double-check information when updating personal data

Administrative tasks could involve sending information to other organisations or emailing parents/carers with sensitive information about their child. To avoid sharing information with an incorrect party, consider implementing a process to double-check you have the correct recipient and address.

2. Disable autofill in your email settings

If people's email addresses come up automatically when starting a new email message then you have autofill enabled in your settings. While this tool might save time, you could be more at risk of sending an email to the wrong person by mistake (especially if email addresses are similar), so it's a good idea to disable it.

3. Ensure staff receive the relevant training

Emphasise the importance of good data protection to all staff, in particular your support staff who will handle data as part of their role. Data Protection training needs to be part of all staff induction and should be incorporated into regular training, to reduce the number of administrative errors and personal data breaches.

4. Implement appropriate access controls

Consider limiting access to information held in your systems. Review the technical controls you have in place to ensure that personal data is not made available to any staff who do not require access to it. Access to personal data should be granted to staff in line with their role within your organisation. Staff should have their own unique log-ins and passwords and these shouldn't be shared with each other. If IT access is monitored staff should also be made aware of this.

5. Treat data in confidence

Make staff aware of their responsibility to keep information confidential. You should include this in any contract of employment. Idle chit-chat and the verbal exchange of information regarding colleagues or students could be considered as a personal data breach. Educational settings handle very sensitive and delicate issues. Staff should be professional at all times and consider the implications of discussing information relating to staff, students and others they come into contact with.

6. Consider how to keep data secure

In a busy learning environment where staff and students move around regularly, it can be easy to misplace files and keep devices secure. Staff should be aware of their responsibilities in ensuring that all data is kept safe and secure; computers should be security protected, paper files should be locked away and not left around on office desks or on photocopiers and printers. The site should be secure at all times to avoid theft and unauthorised access to IT equipment and data.

7. Keep your IT systems up-to-date

Schools and other educational settings hold lots of data, which means they can be extremely vulnerable to cyber security breaches. You can reduce your risk of cyber threats, such as attacks on computer systems, by making sure you regularly install security updates. You may find our Ransomware and Data Protection Compliance guidance useful.

8. Use blind carbon copy when sending emails

You should ensure that staff are aware of how and when to blind copy email recipients. Ensure that staff receive sufficient training on how to use this tool to prevent email addresses from being visible to other recipients.