

[REDACTED]

---

**From:** ICO Casework <icocasework@ico.org.uk>  
**Sent:** 24 March 2022 17:01  
**To:** [REDACTED]  
**Subject:** ICO Decision - IC-159423-N9G8

## **Reference Number IC-159423-N9G8**

Dear [REDACTED],

I am writing further to your personal data breach report of 4 March 2022 regarding the student who accessed a Webinar using an app via mobile and that names and email addresses were visible.

Thank you for the information you have provided.

### **Data security requirements**

You are required to have appropriate technical and organisational measures in place to ensure the security of personal data.

### **Our Decision**

We have considered the information you have provided and we have decided that no further action by the ICO is necessary on this occasion. This decision is based on the information we have recorded about the breach.

The reasons for our decision are as follows:

- Belfast Recovery College blind carbon copies all students in courses. This action took place for this course to protect confidentiality.
- It was discovered for the first time that names and emails appeared to be visible using an app via their mobile but when a PC or laptop is used this appears not to be the case.
- Action was taken by the team leader on the date of the discovery of the breach which included investigating the incident and contacting the IT department for advice.
- The staff member had received data protection training in the last two years.
- Since the breach Webinars have been temporarily postponed until the IT department can resolve the issue. You will also be giving refresher training for staff on Microsoft Teams and your Standard Operating Procedures will be reviewed and revised to ensure student confidentiality. A cycle of audits will be established on completion of this.

However, we recommend that you investigate the root causes of this incident to ensure that you understand how and why it occurred, and what steps you need to take to prevent it from happening again.

In particular, we recommend that you consider:

-Ensuring the verification and checking measures you have in place are sufficiently robust in order to mitigate a future occurrence.

-When introducing any changes to your systems, robust penetration and security testing should be carried out prior to going live, to ensure that the system is fit for purpose.

-Ensuring that periodic further checks and reviews are made to maintain the effectiveness and confidentiality of the system.

The ICO recognises the unprecedented challenges many organisations are facing during the Coronavirus (COVID-19) pandemic, and are reflecting this in our processes. We understand that in some cases, resources might be diverted away from usual compliance or information governance work. We fully understand this may lead to a delay in your investigation being completed and implementation of the recommendations listed. Therefore, we ask you to complete them as soon as you are able to, as this will help to protect the personal data you hold from similar occurrences in future.

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

Please also note that as a result of a breach an organisation may experience a higher volume of complaints and information rights requests. You should not refer them to the ICO as a matter of course, and it is important that you deal with these, alongside the other work that has been generated as a result of the breach.

Thank you for reporting the incident. Further information and guidance relating to [data security](#) is available on our website.

We now consider the matter to be closed.

Yours sincerely

Simon Andrews  
Lead Case Officer  
0330 414 6498

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

Ref No:	Date	Risk/ Area	Progress	Actioned by	Status	Comments (Further Issues Identified & Considerations)
1	24.2.2022 3pm 25.2.2022	Report by student having difficulty accessing webinar. Report that student emails addresses are visible in MS teams meeting accessing via an app.	<ul style="list-style-type: none"> <li>Information Technology Section contacted for advice immediately.</li> <li>Investigation by RC TL &amp; IT</li> <li>Temporary postponement of courses to resolve issue on 3.3.2022</li> <li>Meeting with IT on 8.3.2022 to review issue and provide guidance to prevent further DP risk and investigate scale.</li> </ul>	RC / IT Team	RAG	<ul style="list-style-type: none"> <li>Daily emails to resolve issue</li> <li>Investigation clarified if bcc used - yes</li> <li>Individuals impacted in this course – 29 possible.</li> <li>Option as joining as guest prevents activity reporting in Trust</li> <li>New standard operating procedures required on resolution</li> <li>Training by IT</li> <li>User Education</li> <li>Wider Trust issue?</li> <li>Zoom investigated as not used in Trust.</li> <li>Regional Plan – M Teams via BSO</li> </ul>
2	3.3.2022	ICO report required.	<ul style="list-style-type: none"> <li>ICO Notification drafted for sign off by senior management / Completed with mitigations and actions.</li> <li>Reviewed by DP Dept. and submitted 4.3.2022</li> </ul>	Co-Lead RC / Co Director to approve		<ul style="list-style-type: none"> <li>Advice on threshold and consider whether data subjects are told at this stage – No as not totally quantified to date.</li> </ul>
3	8.3.2022	Meeting with IT and Technical Team	<ul style="list-style-type: none"> <li>Follow – up meeting on 9.3.2022</li> <li>Interim solution by IT – RC TL issues email to students to advise issues with Teams and sending links to Belfast Trust emails. Requests to use personal emails.</li> </ul>	IT & RC Team		<ul style="list-style-type: none"> <li>New issue – Students who have downloaded app or who have MS Teams in their own organisation – ongoing issues with visibility of email.</li> </ul>

			<ul style="list-style-type: none"> <li>Chat function disabled from 21.3.2022 onwards to x</li> </ul>			
4	11.3.2022	Internal Datix Incident Form	<ul style="list-style-type: none"> <li>Datix approvals sought from IT</li> <li>Completed by RC – staff member who discovered incident</li> </ul>	RC Team		Incident Number created
5	16.3.2022	Draft letter with explanation and current actions to student identified issue and current workaround.	<ul style="list-style-type: none"> <li>Letter completed and send for sign off by senior management.</li> </ul>	RC Team		
6	22.3.2022	Letter approved	<ul style="list-style-type: none"> <li>Letter emailed by DP Dept with in time-scales (25.3.2022)</li> </ul>	DP Manager / Team		
7	22.3.2022	Feedback from student raising issue that session attended on 10.3.2022 – chat still visible.	<ul style="list-style-type: none"> <li>Disable the chat function on 25<sup>th</sup> March.</li> <li>Ascertain screen shots.</li> <li>Co –Director instructs chat to be disabled until resolution with IT.</li> </ul>	IT Team advised chat function can be disabled in meeting options. Enabled again on 8 <sup>th</sup> April		<ul style="list-style-type: none"> <li>If student makes chat available it is in the public domain already and may not be a data breach? To be checked.</li> </ul>
8	23.3.2022	Student advised that they have option of deleting own chat.	<ul style="list-style-type: none"> <li>DP Dept sent email advising student.</li> </ul>	DP Team / Manager		

Action Plan (IT/RC and DP)

Microsoft Teams – Data Breach

Updated 20.5.2022

9	23.3.2022	Student advises that chat is accessible from previous courses. Question – is it a permanent record?	<ul style="list-style-type: none"> <li>Telephone call / Email with IT to discuss if previous chats from previous courses can be deleted</li> <li>Gather info to carry out a test by IT – How joining meetings? Desktop, app, mobile phone, using a personal teams account or guest?</li> </ul>	RC TL to call IT IT to test.	<ul style="list-style-type: none"> <li>How long (+ resources) will it take to delete previous chats if over a significant period and how can this be done?</li> </ul>
10	23.3.2022	IT advises that attendees can see previous chats because they joined with their Trust accounts.	<ul style="list-style-type: none"> <li>Information gathered and test to be carried out by IT</li> </ul>	IT	Process to shut down course and put in a lobby to prevent access
11	24.3.2022	It is possible to go back into historic meetings and to chat, see email addresses?	<ul style="list-style-type: none"> <li>Process to shut down Course and put in a lobby to prevent access</li> </ul>	IT	Some courses cannot be shut down, as the staff member who set up the courses no longer work in the trust. This has been escalated within Microsoft on a number of occasions. It is subject to ongoing investigation and a further update will be provided when received from Microsoft
12	24.3.2022	Examine privacy policy of Trust	<ul style="list-style-type: none"> <li>Trust privacy policy in place for students but not readily advised or signposted to.</li> </ul>	RC Team tasked to draft / coordinate for approval.	Will Trust privacy policy cover this issue from RC or others providing MS Teams education classes?
13	24.3.2022	Privacy policy may not accurately reflect use of personal data	<ul style="list-style-type: none"> <li>Privacy Policy to be reviewed in light of breach</li> </ul>	To be approved by senior management.	
14	24.3.2022	ICO reviewed issue and satisfied with response to date, but have set out actions for the Trust.	<ul style="list-style-type: none"> <li>Mitigations to prevent future issues</li> <li>Security testing prior to going live and periodic checks to check workarounds working.</li> </ul>	IT	

15	24.3.2022	Student advises that emails still visible	<ul style="list-style-type: none"> <li>Asked for screen shot but none received to check issue</li> </ul>	IT / RC Team	
16	25.3.2022	Team Lead puts together guidance for admin staff to IT for approval to test.	<ul style="list-style-type: none"> <li>IT tested 11.41 am and guide worked fine.</li> <li>Further round of testing carried out by IT and working. 15.20pm</li> </ul>	IT Team	
17	29.3.2022	Can access to chat be removed urgently – DP	<ul style="list-style-type: none"> <li>DP Manager to identify if one meeting or more.</li> <li>09.19am – IT advises piece of work being carried out to ascertain if previous chats can be deleted from current historic courses.</li> <li>Date of meeting needs to be supplied by student so correct chat is deleted.</li> <li>12.11 IT K to contact to change settings on this meeting to prevent students joining meeting without being admitted and remain in lobby.</li> </ul>	DP Manager IT Team	Difficulty with retrospective history but system moving forward is possible. All options to be explored IT not clear if they can change settings on past meeting. This has been escalated within Microsoft on a number of occasions. It is subject to ongoing investigation and a further update will be provided when received from Microsoft
18	29.3.2022	RC Co Lead requests review of issues and if zoom can be used as interim measure.	<ul style="list-style-type: none"> <li>IT to investigate</li> </ul>	IT Team	Advised not possible as regional move to zoom
19	30.3.2022	Staff provided with interim instructions as advised by IT to continue service of Webinars	<ul style="list-style-type: none"> <li>Admin staff to follow instructions.</li> </ul>	Admin staff RC	
20	31.3.2022	Review by IT advising that MS Teams no longer appropriate in its current form for education classes.	<ul style="list-style-type: none"> <li>IT to review urgently and take into account for full organisation.</li> </ul>	IT Team	
21	6.4.2022	Other students not yet aware of data breach due to IT investigation of issues and support from Microsoft	<ul style="list-style-type: none"> <li>Letter to be drafted to inform students of data breach and impact.</li> </ul>	RC Team	Provided to IT to check technical accuracy correct. All to sign letter off and corrections to be made.

22	6.4.2022	FOI		<ul style="list-style-type: none"> <li>Provision granted</li> </ul>	DP Team / RC Co Lead	
23	6.4.2022	ICO requires update – fuller extent of findings from original investigation. Up to 1000 attendees may have seen email addressed to other attendees. Chats still accessible but put up by attendees in chat room and only those in ms teams could see this. Advised as first complaint in 2 years that considered no risk of harm to attendees.	<ul style="list-style-type: none"> <li>DP Manager contacted ICO by telephone to update issues and scale 6.4.2022</li> <li>To advise that an ongoing action plan was in place to document actions</li> </ul>	DP Manager	ICO advised no requirement to resubmit and that the action plan was sufficient at this time rather than submitting a second incident form.	
24	6.4.2022	SAR Request on personal information in RC	<ul style="list-style-type: none"> <li>Information to be supplied to DP Department</li> </ul>	RC Team and DP Manager		
25	7.4.2022	Public Liaison FOI	<ul style="list-style-type: none"> <li>Response to be made by 25.4.2022</li> </ul>	8D - IT Lead RC – Co lead		
26	7.4.2022	Advise students with final letter	<ul style="list-style-type: none"> <li>Coordinate responses</li> <li>Dispatch letter Easter week</li> <li>PK to set up separate email accounts for 4 staff to access and easiest way to dispatch.</li> <li>Final sign off of letter by all.</li> <li>Email 14.4.2022 to ask for sign off</li> </ul>	RC Team to coordinate amends to draft letter. <ul style="list-style-type: none"> <li>RC T to dispatch</li> <li>IT (new general email account)</li> </ul>	<p>Separate emails created by 13.4.2022 to dispatch letter.</p> <p>Further feedback from IT K on 13.4.2022 to check an area.</p> <p>14.4.2022 Sign off given by all.</p> <p>1.4.2022 – IT advises M365 with 500 – recipients per email.</p>	
27	7.4.2022	Teams Forms – Shared email	<ul style="list-style-type: none"> <li>IT to examine change from JM using Microsoft Flow</li> </ul>	RC / IT Team	Issues / Microsoft Flow	
28	8.4.2022	Staff who have left Trust set up meetings – No access to close meetings so no access.	<ul style="list-style-type: none"> <li>IT 8D approved IT to action.</li> <li>IT 8D approved and Co Director/ IAO</li> <li>PK to re-enable accounts</li> </ul>	IT Co-Director RC Co lead RC B7	Issues with admin getting access to close meetings – error messages appearing.	

29	13.4.2022	Review Meeting by All Privacy Policy Student Charter Layering approach Email invite Historic Meetings	<ul style="list-style-type: none"> <li>Admin to close down MS Teams Meeting to restrict access to previous chats.</li> <li>Permission to be sought from staff on leave</li> <li>Privacy Policy to be developed / updated – RC to draft for approval.</li> <li>Student Charter</li> <li>Structure of RC</li> <li>Historic Meetings – Microsoft meeting</li> <li>Email invite</li> <li>Recording emails to date</li> <li>FOI</li> <li>Coordinate action plan</li> </ul>	RC Team IT Team DP & IT RC Co Lead to approve.	Email invite and guidance completed and updated and final guidance sent 29.4.2022 for sign off and approved on 29.4.2022
30	13.4.2022	Historic Courses – Ability to close down from meeting organisers who left Trust	<ul style="list-style-type: none"> <li>Microsoft to be contacted by IT</li> </ul>	IT Team	
31	14.4.2022	New additional issue - Student using a business / organisational email address in or out of the Trust are able to view other emails who have an MS Teams Account.	<ul style="list-style-type: none"> <li>Form of words by IT to assist in email communications</li> </ul>	IT Team	“In cognito and In Private web browser and to use personal email if they do not wish their email to be viewed. Agreed 29.4.2022
32	27.4.2022	Draft Privacy Policy	<ul style="list-style-type: none"> <li>RC to send to DP</li> </ul>	RC Team	
33	28.4.2022	Draft Privacy Policy Student Charter	<ul style="list-style-type: none"> <li>RC send for comments</li> </ul>	RC Team	Final comments received 3.5.2022
34	29.4.2022	Coordinate actions from all for action plan	<ul style="list-style-type: none"> <li>RC to coordinate and produce draft</li> </ul>	RC Team	Prioritise emails, privacy policy, student charter
35	29.4.2022	Communication to Trust	<ul style="list-style-type: none"> <li>Resources from IT to publicise in the IG bulletin and guidance to Trust</li> </ul>	IT Team	

**Action Plan (IT/RC and DP)**

**Microsoft Teams – Data Breach**

**Updated 20.5.2022**

36	29.4.2022	Guidance to students on MS Teams via email	IT and RC TL to develop	IT / RC Team	Completed.
37	3.5.2022	Student Charter – Communication in easy format to students to make data management clear and what students are signing up for in MS Teams	RC to take amends on student charter	RC Team	Sign off on 3.5.2022
38	3.5.2022	Regional feedback required for HSC organisations RE: Regional roll out of MS Teams and lessons learnt for others	<ul style="list-style-type: none"> <li>Advise BSO IT who are rolling out MS Teams regionally for wider lessons learned and integrate issues / solutions into wider regional planning for MS Teams.</li> <li>Advise retention policy issue</li> <li>Ask for BSO IT feedback if can offer any resolution / suggestions.</li> </ul>	DP Team	<ul style="list-style-type: none"> <li>Issues advised. Security issues with mobile apps</li> <li>MS Teams meeting cannot be deleted once over – meeting needs to be closed.</li> <li>Retention policy issues for past meetings – users can go back into previous meetings and Trust cannot take any action or resolve.</li> <li>If meeting set up by an organiser who has left Trust and login created, meeting / course cannot be located.</li> </ul>

**Key:**

DP – Data Protection Team / Manager

IT – Information Technology Team

RC – Recovery College

RC Co Lead – Recovery College Co-Lead

IT 8D – Information Technology Trust Lead