

## Potential Personal Data Breach

I attach copies of correspondence by email between the Complainant and the single point of contact with regard to his complaint. We were told by him, in January, that he had made a complaint but he refused to tell us what the specifics of the complaint were. This was during the employment of our ex-clerk

When I (as voluntary acting clerk/assistant) received the forwarded correspondence in May I removed from the Parish Council website all the old registers of interest which I believed, from reading the complaint papers, were the cause of the complaint. That was the whole extent of my actions in response.



THIS PAGE WAS A CONTROLLED DOCUMENT

THIS PAGE CONTAINED A CONTROLLED DOCUMENT

ICO Officer Email

**From:** ICO Casework

**Sent:** 21 April 2021 15:03

**To:** CCC Employee Details

<[REDACTED]>

**Subject:** ICO Case Reference: IC-83140-Y7H9

21st April 2021

**Case Reference: IC-83140-Y7H9**

Good Afternoon,

Please find attached details of a data protection complaint received by the ICO regarding St Cleer Parish Council and the action you should take in response to this complaint.

Yours sincerely,

ICO Officer Details

Case Officer  
Information Commissioner's Office

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF  
T. 330 414 6774 [ico.org.uk](http://ico.org.uk) [twitter.com/iconews](https://twitter.com/iconews)  
Please consider the environment before printing this email.

For information about what we do with personal data see our privacy notice at  
[www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice).

This e-mail and attachments are intended for above named only and may be confidential. If they have come to you in error you must take no action based on them, nor must you copy or show them to anyone; please e-mail us immediately at [enquiries@cornwall.gov.uk](mailto:enquiries@cornwall.gov.uk). Please note that this e-mail may be subject to recording and/or monitoring in accordance with the relevant legislation and may need to be disclosed under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004. Security Warning: It is the responsibility of the recipient to ensure that this e-mail and any attachments are virus free. The Authority will not accept liability for any damage caused by a virus.

THIS PAGE WAS BLANK

St Cleer Parish Council  
The Sports Pavilion,  
Hockings House,  
St Cleer,  
Cornwall,  
PL14 6EE

21<sup>st</sup> April 2021

**Case Reference: IC-83140-Y7H9**

Dear Chief Executive,

The Information Commissioner's Office (ICO) has received a complaint about the way your organisation processes personal data. We received the complaint from [REDACTED] on 12<sup>th</sup> January 2021 and I have attached the relevant details.

### **The ICO's role**

Our role is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

One way that we do that is to consider complaints from individuals who believe there has been an infringement of the data protection law. Section 165 of the Data Protection Act 2018 requires us to take steps to respond to the complaint including investigating it to the extent that we feel is appropriate and informing the complainant of the outcome.

### **The outcome of this complaint**

[REDACTED] has complained to the ICO about your handling of their data protection complaint. They believe that you have not complied with your obligations under data protection legislation.

**It is our decision that there is more work for you to do and now expect you to take steps to address any outstanding issues with your [REDACTED]**

### **What you need to do now**

One of the ICO's strategic goals is to increase the public's trust and confidence in how their personal data is used and made available and this relies on data controllers being accountable for their

actions in relation to handling data and responding to information rights requests.

Accountability is one of the data protection principles and makes you responsible for complying with the General Data Protection Regulation (GDPR).

You must be able to demonstrate your compliance to the complainant and work hard to promote trust and resolve their concerns without the need for the individual to come to us. The attached document provides more detail about this.

As a regulator we look to organisations to effectively manage and resolve the data protection complaints they receive. When a complainant comes to us to complain, they are in effect telling the regulator that they believe you are breaking the law. Reports of this kind are something that we will treat seriously and robustly.

We do not expect to receive complaints when there is still further work that you can do to better explain the processing in question to the complainant, or to put things right when they have gone wrong.

We therefore require you to revisit the way you have handled this matter and consider what further action you can now take to resolve this complaint. We expect organisations to deal with the data protection complaints they receive and to proactively work with complainants to provide an appropriate resolution.

If you believe that you have complied with the data protection law, you need to explain this in detail to Mr Johnson. You also need to be confident that you have done all you can to find an appropriate resolution. If your organisation could have done more to resolve the concern then we expect you to take steps now to resolve the issue with the complainant.

I have included a checklist in the attached document to help you with this, you should be able to tick off all the points on this non exhaustive list.

We expect you to contact [REDACTED] within the next **28 days** with this further detail. If you are unable to meet this timeframe we expect you to contact him to let him know and to advise Mr Johnson when to expect it. You do not need to provide a response to us at this stage.

However, if we receive a further complaint about this processing, we will carefully review and assess the response you have provided



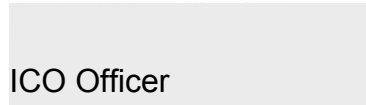
to the complainant. If we consider that you are infringing data protection law then we will consider using our formal powers and any sanctions available.

Although individuals do have the right to raise complaints with the ICO, we should not be viewed as a routine second stage in a resolution process. As indicated above, we expect organisations to take their personal data obligations seriously and this should reduce the need for individuals to approach the regulator directly.

### **Advice and assistance**

Our website contains advice and guidance about the processing of personal data and an organisation's obligations under the Data Protection law. I recommend that you review the information on our website to fully understand your obligations and in particular our [accountability framework](#). We also have specific information about [how you should respond to data protection complaints](#).

Yours sincerely,



ICO Officer

Please consider the environment before printing this email.  
For information about what we do with personal data see our [privacy notice](#).

### **ICO Statement**

You should be aware that the Information Commissioner often receives request for copies of the letters we send and receive when dealing with casework. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do.

THIS PAGE WAS BLANK

## **Accountability – guide for organisations**

### **Accountability – what is it?**

Accountability is one of the key principles in data protection law – it makes you responsible for complying with the legislation and says that you must be able to demonstrate your compliance.

Accountability means putting in place appropriate and effective policies, procedures and measures. Accountability enables you to develop people's trust in how you use their personal data and plays a part in their overall confidence and support for your services. You can find more information about [accountability and governance](#) on our website.

### **The accountability framework**

The ICO has developed an [accountability framework](#) which is available on our website and is aimed at helping organisations to comply with their obligations. It sets out expectations and examples of how organisations can demonstrate accountability and is a useful tool to use. We recommend that you use the framework. The [accountability self-assessment](#) will help you to assess the extent to which your organisation is currently meeting the ICO's expectations in relation to accountability.

### **Accountability – how it fits in with our complaint handling process**

The ICO's role is "to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals". As a regulator, our primary responsibility is to ensure compliance with the law.

One way that we do this is by gathering and dealing with complaints brought to us by members of the public, with the overall aim of improving organisations' information rights practices.

When someone complains to the ICO they're essentially telling us that they believe that an organisation has not complied with data protection law.

We are here to ensure that organisations take their responsibilities under the Data Protection Act seriously. That means we expect organisations to work with those that raise complaints. You need to be clear about how you have processed their personal data, and how you have fully complied with the law and your obligations. This might mean you have to offer more than one explanation for the actions you have taken. Individuals do have the right to complain to the ICO but organisations should want this to be a last resort and not something that happens as a matter of routine.

Our casework approach puts the onus on organisations to remedy their customer's complaint. The accountability principle means that organisations should be able to demonstrate to their customer and us, how they have complied with the legislation.

### **What do we do with organisations that don't comply with the law?**

We will continue to use the complaints that we receive to help us to decide when it's right for us to take stronger action.

We will use the tools available to us to help us to build up a picture of which organisations we receive complaints about, which are flouting the DPA and which may simply need some more help. This will enable us to shape our approach – some organisations may need us to signpost them to information on our website, others may be ones that we consider taking stronger regulatory action. Any decisions to take regulatory action will be done in line with the Regulatory Action Policy (RAP)

### **What do we need you to do?**

If we receive a data protection complaint about your organisation we will write to you with the details and ask you to look into it. It is your responsibility to explain to your customer how you have complied with the law, or if something has gone wrong, to outline the steps taken to put it right.

- As a regulator we look to organisations to effectively manage and resolve the data protection complaints they receive. We do not expect to receive complaints when there is still further work that can be done to help to resolve the problem.
- When your customer comes to us to complain that you are breaking the law this is something that we will treat seriously and robustly.

If you feel that you have complied with data protection law but your customer disagrees you need to explain to your customer in as much detail as you can, why this is. You also need to be confident that you have done all you can to find an appropriate resolution.

The following checklist will help you ensure you have done everything you can to resolve your customer's complaint. You should be able to tick off all the points on this list.

One of the ICO's strategic goals is to increase the public's trust and confidence in how their personal data is used and made available. **You can help with that in ensuring that you explain fully, to the data subject, how you are complying with your obligations under the law.**

## **CHECKLIST -responding to data protection complaints**

- ☐ We have fully investigated the data protection complaint made by our customer.
- ☐ We have referred to and used ICO guidance to help us respond and deal with the issues raised.
- ☐ We have used the accountability self-assessment framework to assess if we are currently meeting the ICO's expectations.
- ☐ We have provided a detailed response to our customer including:
  - An explanation of the parts of the legislation that apply to the complaint.
  - If something has gone wrong, what we have done to put it right including offering compensation if it's appropriate.
  - If we have complied then we've properly explained the parts of the legislation that allow us to process information in the way we have done.
  - Where appropriate, we have issued a final response/deadlock letter (see below).
- ☐ We have done what we can to prevent a complaint from being escalated to the ICO.
- ☐ If a complaint is raised with the ICO we can:
  - Show that we have complied with the legislation and that we have properly engaged with our customer in line with the accountability principle in the legislation; or
  - Show that we have acted to improve our processing, correcting any shortcomings and that we have properly engaged with our customer in line with the accountability principle in the legislation.

### **Final response letter**

**Organisations should be clear to individuals when they have done everything they can to resolve their complaint. This could involve issuing a final response/deadlock letter that sets out what you have done to address the complaint in detail, and next steps.**

THIS PAGE WAS BLANK

Interview Date: 12/01/2021 15:42:45

Field	Value
Sequence ID	DPCM-00033536
Retention schedule	-
About your complaint	-
What is your complaint about?	The way an organisation is handling/processing my personal information
What is your complaint? The organisation ...	-
What is your complaint? The organisation ...	Something else
Please give details	This is a notification of a potential personal data breach of a 3rd party where the 3rd party data is compromised at a parish council webpage. Initial contact with the PC requesting the details of a nominated data protection individual resulted in being referred to a county council point of contact where that point of contact returned an out of office response by email. A subsequent email from the county council ignores the request for a nominated data protection individual and recommends referring the matter to the ICO. The potential breach is the publication of personal signature (protected data) of a serving parish councillor at the parish council webpage where name address and personal details are also published. Whereas some data is necessarily published, a personal signature should be redacted. The webpage link is <a href="http://www.stcleerparishcouncil.gov.uk/_UserFiles/Files/_People/-Pete_Nash_ROI.pdf">http://www.stcleerparishcouncil.gov.uk/_UserFiles/Files/_People/-Pete_Nash_ROI.pdf</a> which displays a personal signature for 1 individual whereas all other such documents for a dozen or so other councillors are redacted.
Supporting document	a5ce2478-c35e-4822-8045-8172df55c4d3\1 St Cleer PC Personal Data Breach Administrative failure.pdf
Supporting document type	Response from organisation
Add another	True
Document 2	40f69952-037c-4f34-9e29-8dfc65b36187\2 Automatic reply St Cleer PC Personal Data Breach Administrative failure.pdf
Supporting document type	Response from organisation
Add another	True
Document 3	1d0d94f8-defa-41a3-b9be-75a10c43c895\3 St Cleer PC Personal Data Breach Administrative failure.pdf
Supporting document type	Response from organisation
Add another	True
Document 4	ccba71ed-c950-414b-830a-ea870b0a72bd\4 St Cleer PC Personal Data Breach Administrative failure.pdf
Supporting document type	Response from organisation
Supporting evidence summary	1 Initial notification to PC of potential data breach 2 Out of office response from county council 3 Response from parish council 4 Response from county council
What more could the organisation you're complaining about do to resolve your complaint?	Acknowledge the seriousness and immediacy of dealing with a reported potential personal data breach and notify a suitable data protection individual so that information could be passed to investigate and remedy the situation in a professional and timely manner
Organisation your complaint is about	-
Organisation name	St Cleer parish council
Organisation address	-
Address	GB
Contact name	Chairman of the Parish council J Prin

Field	Value
Email	
Phone	PERSONAL TELEPHONE NUMBER
About you	-
First name	
Last name	
I'm acting on behalf of someone else	False
Name of person you are acting on behalf of	-
Authority to act on behalf	-
Supporting document type	Authority to act on behalf
I/person making this complaint was 16 or under	False
Your email	PERSONAL EMAIL ADDRESS
Your address	-
Address	GB
Phone	
Declaration	-
I understand that the ICO may need to share the information I have provided so they can look into my complaint, and have indicated any information or documents that I don't want the ICO to share. I understand the ICO will keep the information relating to my complaint, including any documents for two years, or longer if necessary. If I am making a complaint on someone else's behalf, I confirm that I am allowed to act on their behalf.	True



From: [REDACTED] PERSONAL EMAIL ADDRESS  
Subject: St Cleer PC - Personal Data Breach / Administrative failure  
Date: 11 January 2021 at 10:09  
To: J [REDACTED]  
Cc: enquiries@cornwallalc.org.uk

This correspondence is directed at the Chair of St Cleer PC, the Chair of St Cleer PC Assets committee and the Acting Clerk for their direct personal attention and action.

It is additionally copied to Cornwall council and the Cornwall Association of Local Councils on the basis that both organisations are providing regulatory advice and support to St Cleer PC and that St Cleer PC has a demonstrable record of failure in responding to, and actioning, properly formatted and submitted correspondence.

There are 2 key elements to this correspondence.

The first is to formally notify St Cleer PC that a personal data breach has been identified in relation to a serving St Cleer PC councillor in order that appropriate internal investigation / remediation measures may be initiated and that external reporting of the breach may be completed.

The second is to highlight the recurring failure to publish full, accurate and timely agenda (including supporting documents) for scheduled meetings - in this instance the Estates committee meeting scheduled for 13 Jan 21.

In relation to the personal data breach, in order to minimise the potential for widening the awareness of the breach and exposing the victim to greater potential harm, no further detail will be provided in this correspondence. Detail of the personal data breach will be provided to a single nominated individual with responsibility for data security.

In relation to the repeated failure to publish full, accurate and timely agenda (including supporting documents) for scheduled meetings, this is a consistent and frequently previously highlighted administrative failing by St Cleer PC.

In the current example, there is substantial public interest (as demonstrated by numerous and enthusiastic social media engagement across several outlets) in relation to access the outdoor gym equipment. There are also potential planning applicant(s) (and members of the public who may wish to comment) who are unaware whether their current applications will be discussed or not and there is the obvious inability for any public scrutiny of the scheduled meeting.

Whereas the publication of full, accurate and timely agenda (including supporting documents) should be a cornerstone of simple administrative procedure this is an area where St Cleer PC consistently fail.

Since agenda must be published 5 clear days prior to a meeting and that item(s) not on the agenda may not be discussed, it must follow that either the meeting is cancelled or that there is to be no discussion.

This is a repeat example of previously reported and recorded systemic administrative failure which is characteristic of St Cleer PC. The administrative failure is amplified by the concurrent, repeated failure to publish minutes of previous meetings - the latest manifestation being the absence of minutes for the 25 Nov 20 PC meeting at the St Cleer PC webpage.

## Employee Personal Details

### Action:

- St Cleer PC is formally notified of a personal data breach in relation to a serving councillor. There are time sensitive Statutory requirements which follow such notice.
- St Cleer PC is formally notified of the requirement to publish full, accurate and timely agenda (including supporting documents) for scheduled meetings and that no item may be discussed which is not on the agenda. Further, all minutes must be published within 30 days of the date of a meeting whether ratified or not.

### Info:

Cornwall council and Cornwall Association of Local Councils - as organisations providing external advice, guidance and oversight to St Cleer PC.

THIS PAGE WAS BLANK

From: CCC Employee details  
Subject: Automatic reply: St Cleer PC - Personal Data Breach / Administrative failure  
Date: 11 January 2021 at 10:09  
To: [REDACTED] PERSONAL EMAILADDRESS



I am out of office, please redirect emails to: CCC Employee

This e-mail and attachments are intended for above named only and may be confidential. If they have come to you in error you must take no action based on them, nor must you copy or show them to anyone; please e-mail us immediately at [enquiries@cornwall.gov.uk](mailto:enquiries@cornwall.gov.uk). Please note that this e-mail may be subject to recording and/or monitoring in accordance with the relevant legislation and may need to be disclosed under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004. Security Warning: It is the responsibility of the recipient to ensure that this e-mail and any attachments are virus free. The Authority will not accept liability for any damage caused by a virus.

1. The first part of the document is a letter from the author to the reader, explaining the purpose of the study and the methods used. The letter is dated 1998 and is addressed to the reader. The author explains that the study was conducted in order to determine the effect of the new curriculum on the students' learning. The author also explains that the study was conducted in a classroom setting and that the students were given a pre-test and a post-test. The author also explains that the study was conducted in a classroom setting and that the students were given a pre-test and a post-test.

2. The second part of the document is a letter from the author to the reader, explaining the purpose of the study and the methods used. The letter is dated 1998 and is addressed to the reader. The author explains that the study was conducted in order to determine the effect of the new curriculum on the students' learning. The author also explains that the study was conducted in a classroom setting and that the students were given a pre-test and a post-test. The author also explains that the study was conducted in a classroom setting and that the students were given a pre-test and a post-test.

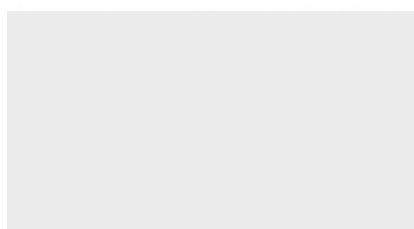
3. The third part of the document is a letter from the author to the reader, explaining the purpose of the study and the methods used. The letter is dated 1998 and is addressed to the reader. The author explains that the study was conducted in order to determine the effect of the new curriculum on the students' learning. The author also explains that the study was conducted in a classroom setting and that the students were given a pre-test and a post-test. The author also explains that the study was conducted in a classroom setting and that the students were given a pre-test and a post-test.

THIS PAGE WAS BLANK

St Cleer PC is duty bound by statutory requirement to expedite an investigate, notification to the victim, remediation and external report to the ICO. Any action / inaction by St Cleer PC may be interpreted by the ICO as unreasonably delaying necessary action.

It may now be apparent to you that I [REDACTED] is out of office but this does not remove the duty under GDPR which rests with St Cleer PC.

KJ

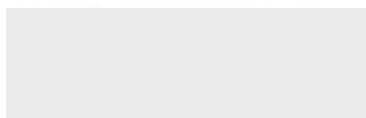


Your single point of contact for the Parish Council is CCC Employee [REDACTED] and I request that you direct your current and all future correspondence to her in this regard

As relates to the meeting of the 13th January this has been postponed.

For information the matter of the outdoor gym is covered by Government Direction.

Yours



Get [Outlook for Android](#)

Commissioner.

I hope that clarifies matters.

Regards

CCC Employee [REDACTED] Corporate and Information  
Governance Manager  
& Data Protection Officer  
Monitoring Officer of the Council of the Isles of Scilly  
Cornwall Council | Corporate and Information Governance  
Legal Services | Assurance

CCC Employee [REDACTED]

[www.cornwall.gov.uk](http://www.cornwall.gov.uk) | 'Onen hag oll'

4th Floor, North Wing, New County Hall, Treyew Road,  
Truro, TR1 3AY

"Cornwall Council's Legal Service will no longer use DX with  
effect from 31 December 2020"

From: [REDACTED]  
[REDACTED] SONAL EMAIL ADDRESS

Sent: 12 January 2021 13:18

To: [REDACTED]

CCC Employee Detail

CornwallALC Enquiries <[enquiries@cornwallalc.org.uk](mailto:enquiries@cornwallalc.org.uk)>;

CCC Employee Details

Subject: Re: St Cleer PC - Personal Data Breach /  
Administrative failure

Dear [REDACTED]

Your request is noted however, I have no interest nor am I  
bound in any respect by policies adopted by St Cleer PC as  
regards points of contact.

I have served notice directly upon you as the Chair and the  
acting Clerk of St Cleer PC notification of a breach of  
personal data in relation to your website.

Thank you for stating the obvious in relation to the relevance, or otherwise, of policies adopted by St Cleer PC in relation to points of contact.

Where contact details for a public body are advertised, or otherwise known, they will be utilised as considered most appropriate to the prevailing circumstance.

As regards the acceptance, or otherwise, of 'responsibility' for action / inaction following a properly notified scenario, the decision of whether appropriate action has followed is not for you, nor St Cleer PC, to decide where a higher authority carries the decision making role - in this case the ICO.

In the absence of a suitable response to the original notification to St Cleer PC (11 Jan 21 10:09) which stated that "... *Detail of the personal data breach will be provided to a single nominated individual with responsibility for data security...*" the matter will be referred to the ICO (as was fully anticipated to be the case.)

In the meantime, and whilst awaiting an **authoritative** decision as to whether a breach has occurred or not, the potential victim will remain exposed and at risk.

Give yourselves a sound pat on the back for a job well done...

[REDACTED]

On 12 Jan 2021, at 13:52, CCC  
Employee Details > wrote:

Dear [REDACTED]

With regards to the content of your email;

Whilst you can opt to ignore the single point of contact that has been set out for you, should you do this the Parish Council will not accept any responsibility for delays in processing any matters which may be relevant.

In considering the alleged data breach; as you have not provided further details the Council does not intend to correspond with you further on this. Should you wish to set out what the breach is you may do so and I will then consider this on behalf of the Parish Council, or you can address your concerns directly to the Information

Controlled Document



From: [REDACTED]

Subject: Data Protection Leak - Due Diligence  
audit required

Date: 13 Jan 2021 at 13:51:07

To: Email Adresses [REDACTED]

Cc: [REDACTED]

Good afternoon

We have been told, quite cryptically, that there has been a data leak made on our website and that this pertains to an active councillor. We have asked for more details but they have not been forthcoming. We do understand that a referral to the Information Commissioner has been made.

May I ask you to review; as a matter of priority that any data about yourself on the website is in accord with your Privacy Statement – I have, to the best of my ability complied with this but I may not be seeing a genuine error myself.

If you do identify any breach of your personal data please can you notify [REDACTED] as a matter of urgency

[REDACTED]

Ben Jones, Clerk

Data Protection / Leak - Due Diligence

and required

13 Jan 2021 at 15:51:07

Marin Eddy

averly@stceparishcouncil.gov.uk,

barag@stceparishcouncil.gov.uk,

beating@stceparishcouncil.gov.uk,

cairgeant@stceparishcouncil.gov.uk,

cullman@stceparishcouncil.gov.uk,

dawson@stceparishcouncil.gov.uk,

guyatt@stceparishcouncil.gov.uk,

john@stceparishcouncil.gov.uk,

parsons@stceparishcouncil.gov.uk,

parry@stceparishcouncil.gov.uk,

sharrod@stceparishcouncil.gov.uk,

snodgrass@stceparishcouncil.gov.uk,

clive.sargeant

Good afternoon

We have been told that you are currently in the process of a data leak on the council website and that this is a serious matter. We have asked if you could provide more details on this and if you could let us know if you are able to provide any further information on this matter.

I am sorry to hear that you are having a difficult time at the moment and that you are not able to provide any further information on this matter. I am sorry to hear that you are having a difficult time at the moment and that you are not able to provide any further information on this matter.

If you are able to provide any further information on this matter, please let us know as soon as possible. We can then provide you with the necessary support and assistance.

Ben Jones, Clerk