

APPENDIX 1

DATA BREACH REPORT FORM

Please act **promptly to report any data breaches**. If you discover a data breach, complete **Section 1** of this form and email it to clerk@cherhillparish.gov.uk

Section 1: Notification of Data Security Breach	To be completed by person reporting incident
Date incident was discovered:	29 August 2026
Date(s) of incident:	29 August 2026
Place of incident:	Cherhill PC laptop communication to councillors
Name of person reporting incident:	Peter Johnson
Contact details of person reporting incident (email address, telephone number):	Clerk@cherhillparish.gov.uk
Brief description of incident or details of the information lost:	Address of a parish resident emailed, at 12.24 pm, by a councillor to Clerk who then, at 14.48 pm, forwarded on to the other 10 councillors, as trusted recipients, for their opinion. The email contained suggestions of anti-social behaviour on the part of the resident.
Number of Data Subjects affected, if known:	Not known
Has any personal data been placed at risk? If, so please provide details:	The resident's home address has been shared. This did not include the resident's name, which is not known.
Brief description of any action taken at the time of discovery:	Discussion by email with the previously appointed Lead Investigation Officer. Followed by an immediate request by DPO to Councillors to delete the email.
For use by the Data Protection Officer	
Received by:	Clerk/DPO
On (date):	30 th August 2026
Forwarded for action to:	Lead Investigation Officer (LIO) and to other councillors for their information.
On (date):	30 th August 2026

Section 2: Assessment of Severity	To be completed by the Lead Investigation Officer
Details of the IT systems, equipment, devices, records involved in the security breach:	One email outlining the information outlined below was sent to the Clerk and one councillor. It was then shared by the Clerk in a subsequent email with all councillors asking them to consider the matter.
Details of information loss:	
What is the nature of the information lost?	The information included a resident's address, speculation as to a medical condition that she may have and speculation as to her relationship with her family. Allegations surrounding the behaviour of her dog.
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	Two emails sent to official Cherill Parish Council email addresses.
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Council or third parties?	The information in the shared emails contain speculation as to a medical condition, i.e. special category data, along with speculation concerning her social / family situation. It may have adverse impacts should it be leaked outside the closed group of councillors to whom it was sent. The unsubstantiated claims may also impact the way the individual is perceived by councillors. It should be noted that the name of the individual is unknown, but her address is recorded.
How many data subjects are affected?	One
Is the data bound by any contractual security arrangements?	No
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas	No
Personal information relating to vulnerable adults and children	Potentially but unknown
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed	Yes – speculation concerning a medical condition and personal family relationships.
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals	No
Security information that would compromise the safety of individuals if disclosed	No

Section 3: Action taken	To be completed by Data Protection Officer and/or Lead Investigation Officer
Incident number	2026/002
Report received by:	Cllr Price
On (date):	31/8/2026
Action taken:	Request that the two emails are deleted by all councillors, and the Clerk, immediately (including sent and deleted mail folders). A response must be given in writing.
Was incident reported to Police?	No
Follow up action required/recommended:	1. If councillors do not respond to the request to delete the email someone with admin access should delete them from the server. 2. Review who successfully completed the previous training. Put an agenda item on each meeting's agenda to review who has not successfully completed the training. 3. Review use of distribution lists for all councillors – does everyone really need to see everything that they do? 4. Establish a practice of appropriately redacting documents / emails etc before they are sent to councillors, or externally. 5. Consider introducing a “two tick” system on all Facebook posts, newsletters, web postings and other external correspondence. 6. Put an item on the next PC meeting agenda to discuss this issue, in general terms, to raise awareness of the problem and seek additional ideas on how to address it.
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO	YES/NO If YES, notified on: Details:
Notification to data subjects	YES/NO If YES, notified on: Details:
Notification to other external agency	YES/NO If YES, notified on: Details: