SHAVINGTON-CUM-GRESTY PARISH COUNCIL

MINUTES OF A MEETING OF THE COMMUNICATIONS COMMITTEE
HELD ON 6 JULY 2018 IN SHAVINGTON VILLAGE HALL, SHAVINGTON

PRESENT: Councillor B Gibbs Chairman
Councillor M Andrews
Councillor W Cooper
Councillor M Ferguson
Councillor K Gibbs

---

26 DECLARATIONS OF INTEREST

Members were invited to make any declarations of interest. The Clerk could offer advice but the decision to declare, or not, was for the parish councillor to decide based on the circumstances.

No declarations were made.

27 DATA PROTECTION ACT 2018

27.1 BREACH NOTIFICATION

As Members were aware, Typeform (a company used by the Parish Council to conduct surveys on its behalf) notified the Council on 29 June 2018 that it had discovered (on 27 June 2018) that an unknown third party had gained access to its server and downloaded certain information, including some of the data supplied by the Parish Council's respondents to surveys undertaken between 2016 and 3 May 2018.

The company took immediate action and closed the source of entry and then carried out a forensic review of all its systems and was now satisfied that all its data was safe.

It was estimated that about 304 of the Parish Council's data subjects might have been affected by the breach.

This took place prior to the introduction of the General Data Protection Regulation (GDPR) which was now enshrined in the Data Protection Act 2018 which, in turn, repealed the Data Protection Act 1998.

27.2 ACTION TAKEN BY THE PARISH COUNCIL

The Information Commissioner's Office (ICO) was notified of the breach on 30 June 2018, using an official notification form from its website.

The form asked for details of proposed action to be taken in the case of a breach. The ICO had been informed that the Parish Council had called an emergency meeting of the Communications Committee to consider future arrangements to mitigate this type of breach by service-providers; a post was to be added to the website; and all affected data subjects were to be notified of the possibility that their data might have been compromised.

27.3 MITIGATION MEASURES

The Committee was invited to consider –

(a) **Mitigation measures to avoid future breaches by service-providers**.

- What can the Council do to reduce the risk of future breaches in data security?
- Should the Council terminate its relationship with Typeform?
  (This would not be able to commence until September when the next edition of the newsletter was issued; the current newsletter made reference to 'Typeform'.)
- Review data security taking into account use of online services.

ACTION AGREED:

(i) Terminate contract with Typeform at the earliest opportunity. Office 365 provided this type of service and included additional security. Microsoft forms, which was part of Office 365, could be used as an alternative.

(ii) Request Typeform to delete all data from its backup systems.

(b) **A method of informing data subjects where there were no contact details.**

ACTION AGREED:

For those individuals whose data had been breached, but for which the Council had no contact details, the breach should be publicised as widely as possible to include social media, the website, minutes and the next issue of the newsletter.

In future, all surveys where data was collected there would be a requirement for respondents to provide contact details in the event of a breach.

(c) **Introduction of a Data Breach Policy**

This should include the following basics:

i. Identifying the nature of the breach and whether there is any potential harm to the individual affected.

ii. Deciding if it is a significant breach. The ICO does not wish to be notified of insignificant breaches. This would, therefore, be a matter of judgement.

iii. Notifying the ICO of the breach within 72 hours of becoming aware of the breach and this must include the number of individuals affected, the categories and approximate number of data records exposed, a description of the likely consequences and measures proposed or taken to mitigate the breach and its possible adverse effects.

iv. Contact data subjects to inform them of the breach.

v. Maintain a log of all breaches.

Members reviewed Part A of Appendix 9 of the GDPR Toolkit provided by the National Association of Local Councils; this was entitled '*Checklist of what to include in a security incident response policy*'. Responses to the questions posed were as follows:

1. The breach response plan

(a) Do you know who should be notified within the council if there is a data breach?

Response: Clerk or Chairman or Vice-Chairman.

(b) What happens if one of your team in (a) above is away on holiday or otherwise absent. Is there a back-up plan?

Response: In the event of one only being unavailable, contact either of the other two.

(c) Do you have clear reporting lines and decision-making responsibility?

Response: Clerk or Chairman or Vice-Chairman.

(d) Do you understand what external assistance you might need, with providers in place in advance?

Response: An Office 365 consultant would be contacted as most breaches would be experienced through the use of Office 365 via Strategy 365 (the Council's partner) and should be able to offer legal advice.

It might also be necessary to use an external contractor, or an independent Data Protection Officer.

(e) Do you have designated person(s) responsible for managing breaches, with full decision-making authority?

Response: Clerk or Chairman or Vice-Chairman.

(f) Do you have processes for triaging incidents, identifying actual breaches and activating the breach response team?

Response: The Communications Committee would act as the response team.

(g) Is your breach response plan up to date?

Response: n/a

(h) Have you tested your breach response plan?

Response: n/a

2.Legal issues

(a) Do you have a process for maintaining legal privilege and confidentiality?

It was understood that this related to communications between a professional **legal** adviser (a solicitor, barrister or attorney) and their clients from being disclosed without the permission of the client.

Response: Process to be considered.

(b) Can you pause document destruction processes?

Response: No provision for this.

(c) Do you have appropriate evidence-gathering capability so you can collect information about the breach?

Response: This is within the Office 365 package.

(d) Do you know who your specialist external lawyers who can manage the investigation and give legal advice are?

Response: Clerk to make enquiries.

(e) Do you have a process for managing and logging steps taken in the investigation?

Response: Template to be prepared.

(f) Do you understand your contractual rights and obligations with third parties?

Response: Yes.

(g) Can you quickly identify third parties you may need to notify?

Response: Yes.

(h) Do you have appropriate contractual rights to be notified of breaches by third parties?

No response given.

(i) Do you know how to contact the Information Commissioners Office ("ICO") and with law enforcement who you can involve quickly if necessary?

Response: Yes

(j) If you hold credit/ debit card data, do you need to notify your payment processor?

Response: n/a

(j) Do you need advice on the legal options available to quickly gather evidence from third parties?

Response: Will need further consideration.

(k) Do you understand your potential liabilities to third parties?

Response: Need to prepare a list of liabilities.

(l) Can you gather information about the breach including taking statements from staff members or councillors who might have seen unusual activity?

Response: Yes

(m) Do you understand when you should consider notifying data subjects and/or regulators?

Response: Yes.

3.Forensic IT

(a) Do you have access to qualified forensic IT capability, either internally or externally?

Response: Office 365 (through Strategy 365).

(b) Do you understand the basic IT do's and don'ts of responding to data breaches?

Response: Yes

(c) Do you have an asset inventory to help you identify potentially compromised devices, where those devices are and in whose possession?

Response: Do not have devices, but all IT services can be suspended if necessary and can 'wipe' devices remotely where Parish Council information is held.

(d) Do you understand how data flows in your council, in practice?

Response: Yes

(e) Can you quickly secure and isolate potentially compromised devices and data, without destroying evidence?

Response: Yes. Can freeze an account to isolate.

(f) Can you quickly ensure physical security of premises?

Response: n/a

4.Cyber breach insurance

(a) Do you have cyber breach insurance, or other insurance which may cover a data breach?

Response: The Clerk to check insurance cover.

(b) Do you understand the process for (a) notifying breaches and (b) obtaining consent for actions from insurers?

Response: Yes

(c) Do you have emergency contact details for your brokers?

Response: Daytime contact details only.

5.Data

(a) Do you know what data you hold (and what you shouldn't hold)?

Response: Checklist to be prepared as part of compliance with Data Protection Act.

(b) Is your data appropriately classified?

Response: Action will need to be taken.

(c) Do you have, and apply, data destruction policies?

Response: There is a document retention policy in existence which will require updating.

(d) Do you know what data is encrypted, how it is encrypted, and when it may be unencrypted on your systems?

Response: All data is encrypted by default.

(e) Do you have regularly check you are complying with your retention policy to ensure you are storing only the data you should be?

Response: Document retention policy to be updated.

(f) Do you have appropriate additional protection for sensitive data?

Response: No.

(g) Do you have data loss prevention or similar tools?

Response: Check tools on the GDPR portal on Office 365.

(h) Do you understand your logs, how long you retain them for and what they can (or cannot) tell you?

Response: Yes. All logged in Office 365.

(i) Do you have appropriate logging of staff/councillor access to data?

Response: Yes

6.Data subjects

(a) Do you understand when you should consider notifying data subjects?

Response: Yes

(b) Do you understand the contractual and legal rights of data subjects?

Response: Yes

(c) Can you quickly prepare appropriately worded notifications to data subjects?

Response: Yes

(d) Do you understand the potential harm to data subjects of loss of the different types of data that you hold?

Response: Yes

(e) Do you have the ability to appropriately triage and deal with a breach?

No response.

(f) Are councillors and staff appropriately trained as to how to deal with data subjects in a breach scenario?

Response: The Council will need guidance on 'do's and don'ts'.

7.Public Relations ('PR')

(a) Do you have access to PR capability experienced in dealing with data breaches?

Response: No.

(b) Do you have template pro-active and re-active press statements?

Response: No template in existence but can be prepared.

(c) Can you actively monitor social media after a breach?

Response: All Communications Committee Members can monitor, together with the Clerk.

RESOLVED: That Appendix 9 (Part A) of the GDPR Toolkit, and the responses, be used as the basis of a Security Incident Response Policy.

27.4 CYBER SECURITY CHECKLIST

The Committee considered Part B of Appendix 9 of the GDPR Toolkit which posed questions in respect of cyber security. The following were the responses.

1 Do you have appropriate policies in place?

a)	Information security policy.	Yes
b)	Privacy policy	Yes
c)	"Bring Your Own Device" ("BYOD") policy	Yes
d)	Remote access policy	Yes
e)	Network security policy	Policy to be prepared
f)	Acceptable use/internet access policy	Policy to be prepared
g)	Email and communication policy	Policies to be prepared.

2. Depending on how your policies are structured, the issues below may appear in one or more of these policies.

a) Are your policies checked and updated on a regular basis and enforced?

b) Is there a council member with responsibility for cyber security?

Response: Councillor B Gibbs.

c) Do you have clear responsibility for cyber security, with clear reporting lines and decision-making authority?

Response: To be decided.

d) Do you ensure physical security of premises?

Response: Yes

e) Do you allocate sufficient budget to cyber security?

Response: Suggested that a sum of £1,000 be allocated in the budget for 2019-2020 for this purpose.

f) Do you subscribe to cyber security updates so that you are aware of threats?

g) Do you have an effective breach response plan, and do you test and update it regularly?

h) Do you have cyber breach insurance in place?

No response.

3. People

a) Do you have appropriate mechanisms for staff and councillors to be able to report suspicious emails quickly and effectively?

Response: Requires further consideration.

b) Do you train staff and councillors on cyber security regularly?

Response: Budget allocation required for 2019-2020 to provide Office 365 training.

c) Do you test staff and councillors, for example by sending spoof phishing emails?

Response: No.

d) Do councillors and staff undertake reviews to ensure that they understand cyber security risks, and are results checked to ensure improvement?

Response: No; will form part of training.

e) Do you have proper processes for when staff or councillors join or leave the council, and are they applied in practice?

Response: Process for new councillors required.

f) Do staff and councillors understand the risks of using public WiFi?

Response: Chairman will provide a list of 'do's and don'ts'.

g) Do you conduct appropriate checks on new staff and councillors to understand if they are a potential security risk?

Response: Not currently carried out for councillors.[1]

4. Hardware, data, encryption and technology

a) Is backup personal data encrypted?

Response: Yes

b) Do you have appropriate mechanisms for securely sending files?

Response: Yes

c) Do you have a list of servers, and individuals who are responsible for ensuring that they are up to date?

Response: n/a

d) Do you have appropriate firewalls and intrusion detection software?

Response: n/a

e) Are your wireless networks appropriately secured?

Response: Yes

f) Do you regularly check the operating systems, data and software against a 'good known state' baseline?

Response: n/a

g) Do you review unsuccessful attacks and probes/scans?

Response: n/a

h) Do you have an inventory (or list of) hardware and software you use?

Response: List required.

i) Do you appropriately limit access to data on a 'need to know' basis?

Response: Share point required.

j) Do you back-up personal data on a regular basis?

Response: No. Office 365 is responsible for all back-ups.

k) Do you apply regular IT updates to your computer hardware and software?

Response: n/a

l) Do you ensure that staff and councillors have anti-virus software loaded and active on their devices at all times?

Response: n/a

[1] Will require clarification. Election of councillors is through the Borough Council and it is Cheshire East Council's role to ensure that candidates are appropriately eligible for election.

m) Do you have appropriate policies regarding use of external hard drives or USB drives?

Response: n/a

n) Do you conduct regular penetration tests and / or red teaming, with appropriate analysis of results?

Response: n/a

5. Third parties

a) Do you properly understand risks arising from third party service providers?

Response: Yes

b) Do you undertake due diligence before engaging third party service providers?

Response: No but is required.

c) Do you assess third parties for cyber security or data protection risks?

Response: No.

d) Do you have obligations in your contracts with third parties requiring them to take steps to keep data secure?

Response: No.

e) If you use cloud storage, do you have contractual rights to be notified quickly of potential security issues?

Response: Yes

6. Remote access/BYOD (Bring your own device)

a) Do you require multifactor authentication where appropriate?

Response: This could be enabled on Office 365 (Strategy 365 to be asked to provide this.)

b) Do you allow remote access?

Response:

c) If so, do you have the right software and controls in place to ensure it is secure?

No Response:

d) Do you have policies to secure mobile devices?

Response: Yes.

e) Is data encrypted on mobile devices?

No Response:

f) Can mobile devices be remotely wiped?

Response: Yes.

g) If you use BYOD, do you apply restrictions to maintain security?

Response: To be considered.

6. User accounts/passwords

a) Do you require unique user accounts?

Response: Yes.

b) Do you require multifactor authentication where appropriate?

Response: Yes.

c) Do you restrict administrator accounts to the minimum necessary?

Response: Yes.

d) Do you require strong, hard to guess, passwords?

Response: Yes.

e) Do you automatically prevent use of common passwords?

Response: Can implement, with a requirement that passwords expire after 180 days.

RESOLVED: That Appendix 9 (Part B) of the GDPR Toolkit, and the responses, be used as the basis of a Cyber Security Policy.

The meeting commenced at 7.15 pm and concluded at 9.00 pm