

ASTON, COTE, SHIFFORD & CHIMNEY PARISH COUNCIL

CLERK'S BRIEFING NOTES

PARISH COUNCIL MEETING ON 5 APRIL 2018

<i>Page</i>	<i>Contents</i>
2	Correspondence sent since last meeting
3 – 4	Councillors' Travel Allowances Scheme 2018/19 (Agenda Item 10h)
5 - 18	GDPR (Agenda Item 8a)
19	Financial Matters: Cash balances at 31 March 2018 (Agenda Item 14a)

Prepared by Helen Sandhu
29 March 2018

Correspondence sent since 1 March 2018

- 1) Letter to St James' Church, containing grant cheque
- 2) Letters to Robert Courts MP, Charles Mathew, Hilary Fenton and Steve Good seeking support for public consultation on Oxford-Cambridge Corridor
- 3) Letter to Steve Neal, Secretary of Aston & Cote Community Trust outlining terms and conditions for potential grant for new playground project

**ASTON, COTE, SHIFFORD & CHIMNEY PARISH COUNCIL
COUNCILLORS' TRAVELLING ALLOWANCES SCHEME
FINANCIAL YEAR 2018/2019**

Aston, Cote, Shifford & Chimney Parish Council, in exercise of the powers conferred by the Local Authorities (Members' Allowances) (England) Regulations 2003, hereby makes the following scheme:

1. Name and Duration

- 1.1. This scheme may be cited as the Aston, Cote, Shifford & Chimney Parish Council Councillors' Travelling Allowances Scheme.
- 1.2. This scheme shall have effect for the period 1 April 2018 to 31 March 2019.

2. Travel and other Expenses

- 2.1. The duties and activities in respect of which travel and related expenses will be payable, are:
 - (a) the attendance at a meeting of the authority or of any committee or sub-committee of the authority, or of any other body to which the authority makes appointments or nominations, or of any committee or sub-committee of such a body, subject to the meeting taking place outside the parish boundary, in accordance with clause 2.9 ;
 - (b) the attendance at a meeting of any association of authorities of which the authority is a member;
 - (c) the performance of any duty in pursuance of any standing order made under section 135 of the Local Government Act 1972 requiring a member or members to be present while tender documents are opened, subject to the venue being outside the parish boundary, in accordance with clause 2.9;
 - (d) attendance at training events and information seminars either organised by the Council or where attendance has been authorised; and
 - (e) the carrying out of any other duty approved by the authority, or any duty of a class so approved, for the purpose of, or in connection with, the discharge of the functions of the authority or any of its committees or sub-committees.
- 2.2. The approval for members to carry out additional duties falling within 2.1(e) above will in general be granted at a previous Parish Council meeting. Where that is not possible, the Clerk, after consultation with the Chairman, has the authority to approve additional duties falling within 2.1(e) above.
- 2.3. A Councillor may be reimbursed for travel and other expenses incurred in connection with or relating to the duties specified in 2.1 above.
- 2.4. Notwithstanding 2.3 above, the following shall be excluded from the scheme in relation to travel and other expenses:

(a) attendance at social events unless this is attendance at such functions as the Parish Council deems it proper for the member to attend as representative of the Council ;

(b) attendance at a meeting of an outside body for which travel and other expenses are paid for by that body

2.5. The rates of the allowances in respect of travel shall be as follows:

All Vehicles Inland Revenue non profit making rate
(currently 45p per mile)

2.6. Taxis should be used, and payment will be made, only where travel by other forms of public transport or by car is not possible.

2.7. Standard class fares only will be reimbursed.

2.8. Related travel expenses, including car parking and road tolls will be reimbursed.

2.9. Travel allowances and related expenses will only be reimbursed for travel or duties undertaken outside the parish boundary.

2.10. In respect of all the claims for travel allowances and related expenses, it is expected that members exercise economy and efficiency, to minimise claims.

3. Claims and Payments

3.1. A claim for travel or other expenses under this scheme shall be made on the claim form designed for the purpose, a copy of which can be obtained from the Clerk.

3.2. A claim for travel or the reimbursement of expenses shall include details of the duty/activity in respect of which the claim has arisen, and a travel claim shall specify the total number of miles travelled.

3.3. A claim for the reimbursement of expenses, shall be supported by a receipt.

4. Publicity

4.1 The Travelling Allowances Scheme will be publicised on the noticeboards in the parish for 14 days after its adoption and will be published on the Parish Council website.

4.2 After the end of each financial year the total amount paid to each member of the Parish Council under the Travelling Allowances Scheme will be publicised on the noticeboards in the parish for 14 days and will be published on the Parish Council website.

4.3 Reports of the Parish Remuneration Panel, a body of the District Council, will be published on the noticeboards and on the Parish Council website.

This allowances scheme was adopted by
Aston, Cote, Shifford & Chimney Parish Council
on (5 April 2018)

ASTON, COTE, SHIFFORD & CHIMNEY PARISH COUNCIL COMPLIANCE WITH GENERAL DATA PROTECTION REGULATIONS 2018

1. Introduction

- 1.1. The General Data Protection Regulations (GDPR) take effect on 25 May 2018. The GDPR replaces the existing law on data protection. The UK's Data Protection Act 2018 is currently going through Parliament (now at the Committee stage).
- 1.2. Many of the concepts and principles of the GDPR are the same as in existing data protection law, but the GDPR places increased emphasis on transparency, openness, the requirement to obtain informed consent to process information and the documentation the Council will need to keep in order to show that the legislation is being complied with. The fines and penalties for non-compliance and data breaches have been substantially increased.
- 1.3. The Parish Council as a corporate body acts as a Data Controller (defined as a body which "determines the purposes and means of the processing of personal data").
- 1.4. Compliance with the GDPR will be monitored by the Information Commissioner's Office (ICO). The Parish Council is already registered with the ICO as a Data Controller.

2. The new six Principles of Data Protection

- 2.1. Fair process – data is processed fairly, lawfully, and in a transparent manner in relation to the data subject
- 2.2. Collected for specific, explicit, legitimate purposes – and not processed further for purposes incompatible with those purposes, or used for any purpose other than that for which it was originally collected
- 2.3. Adequate, relevant and limited to what is necessary
- 2.4. Accurate and, where necessary, up to date
- 2.5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- 2.6. Processed to ensure appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

3. Lawfulness of Processing

- 3.1. Article 6 of the GDPR specifies the restricted reasons for which the processing of personal data is lawful:
 - (a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
 - (b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 - (c) Processing is necessary for compliance with a legal obligation to which the controller is subject;
 - (d) Processing is necessary to protect the vital interests of the data subject or another natural person;
 - (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

- 3.2. Most of the data held and processed by the Parish Council comes under categories (e) and (b).
- 3.3. Should the Parish Council wish to process personal data for different purposes in the future (including for example, obtaining information from a broader section of the public via surveys, questionnaires or other marketing methods), then the Council will first need to review whether the existing policies and procedures (including whether it remains appropriate for the Clerk to act as the Data Protection Officer) will need to be changed.

4. Steps towards Compliance

- 4.1. The ICO has published a checklist for organisations to use to move towards compliance.
- 4.2. The relevant steps for the Parish Council are:
 - Awareness – make sure that decision makers and key people in your organisation are aware that the law is changing;
 - Data audit – document what personal data is held, where it came from, and who it is shared with;
 - Communicate privacy information – review the current privacy notice and change if necessary;
 - Individual's rights – check procedures to ensure that they cover all the rights individuals have, including how personal data would be deleted;
 - Subject access requests – update the procedures and plan how requests will be handled within the new timescales;
 - Lawful basis for processing personal data – identify the lawful basis for each processing activity in the GDPR, document it and update the privacy notice to explain it;
 - Consent – review how you seek, record and manage consent and whether you need to make any changes. Refresh any existing consents if they don't meet the GDPR standard;
 - Children – think about whether new systems need to be put in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity;
 - Data breaches – make sure the right procedures are in place to detect, report and investigate a personal data breach;
 - Data Protection Officer – designate a suitable person/organisation to carry out this role

5. Data Processing by Aston, Cote, Shifford & Chimney Parish Council (ACSCPC) – the Data Audit

- 5.1. ACSCPC processes very little personal data – the data audit carried out by the Clerk has been circulated by email.
- 5.2. ACSCPC does not maintain any lists of personal data (as might be held by an organisation which has a membership body or which has a circulation list for items such as newsletters, for example).
- 5.3. ASCPC does not currently carry out any marketing or other activity in a bid to proactively obtain personal data.
- 5.4. Actions to be taken as identified via data audit:
 - Obtain informed consent from County Councillor and District Councillors for their personal data to be included on the parish council website – will be done via email and retained for record keeping purposes;

- Obtain informed consent from representatives of local organisations whose personal data is included on the parish council website. Will be done via a written form and retained for record keeping purposes. Where consent is withdrawn or no response is received, the data will be removed from the website. The organisations will be contacted to advise them of this. Any new requests for inclusion of personal data on the website will need to be provided on consent form. Copy of consent form attached at Appendix 1.
- Remove data on website relating to local businesses – this data was transferred over from the old website and no requests for no inclusions/updates have been received since it was transferred over. The Parish Council has no evidence of consent having been obtained to publish the data. The Clerk would suggest that it would be unnecessarily onerous to obtain informed consent and to continue to ensure that this data is kept up to date (one of the 6 principles of the GDPR) and the Clerk therefore advises that this data is deleted from the website.

6. Data Protection Officer

- 6.1. As a public authority, the Parish Council is required to appoint a Data Protection Officer (DPO).
- 6.2. The role of the DPO is to monitor compliance with the GDPR and other data protection laws and the organisation's data protection policies, to raise awareness across the organisation of the principles of data protection, to provide training as required, to carry out data protection audits and to be the first point of contact for the supervisory bodies and the individuals whose data is being processed.
- 6.3. The DPO is required to be suitably trained and knowledgeable in data protection law and practices in order to enable them to fulfil the tasks identified in Article 39 of the GDPR (outlined in 5. above). The legislation does not specify the exact credentials and it states that these should be proportionate to the type of processing carried out.
- 6.4. The DPO must be independent. This means that he/she cannot hold a position within the organisation that leads him/her to determine the purposes and the means of the processing of personal data.
- 6.5. The requirement for the DPO to be independent has created some differences of opinion across the local authority sector about whether the Clerk can be the DPO, particularly in smaller councils. The ICO guidance states that in some circumstances it would be acceptable for the Clerk to also act as the Data Protection Officer.
- 6.6. The Clerk has reviewed all of the published guidance, considering how it applies to Aston, Cote, Shifford & Chimney Parish Council specifically, and based on the current volume of and purposes of data processing (as discussed under 3.2 above), the Clerk can be deemed to be sufficiently independent and could act as the DPO. This is because the Clerk does not decide what data to process, nor the means and purposes for which it is processed.
- 6.7. The Clerk has undergone training (with OALC on 14 February 2018) and has read the information provided by NALC, SLCC and the ICO, enabling her to be sufficiently informed on the GDPR and the obligations of a data controller, as is proportionate for the Council.

7. Policies

- 7.1. In order to comply with the GDPR, the Parish Council will need to adopt a some new policies/procedures:
- **Privacy Notice** – draft Notice follows at Appendix 2 for review. This is in the spirit of the GDPR and the UK Data Protection Bill but may be subject to change as the Data Protection Bill goes through parliament. The Parish Council is requested to review and comment and consider for adoption at the May meeting. The Notice would be published on the website.
 - **Data Subject Access Requests** – draft policy/procedure follows at Appendix 3 for review. Again, the Parish Council is requested to review and comment and consider for adoption at the May meeting. This document would be published on the website.
 - **Data Breach Policy and Procedure** – draft policy/procedure follows at Appendix 4 for review. Again, the Parish Council is requested to review and comment and consider for adoption at the May meeting.
 - **Document Retention and Destruction Policy** – to be prepared and presented to the May meeting
 - **Data Security Policy** – to be prepared and presented to the May meeting
 - **Privacy Notice for Staff & Councillors** – to be prepared and presented to the May meeting

8. Website

- 8.1. The AstonOxon website is owned and managed by the Parish Council.
- 8.2. The website contains
- 8.3. many personal records, including:
- The Clerk's contact details;
 - The telephone number of the Chairman of the Parish Council (no contact details for the other councillors);
 - The Register of Member's Interests for each of the councillors;
 - The name, address, email and telephone number of the County Councillor and the District Councillors;
 - The names and contact details for many locally based organisations;
 - The names and contact details for many businesses based in the parish or operated by residents of the parish;
- 8.4. The data from local organisations has often been provided by someone different to the data subject. The Parish Council has not historically sought to obtain formal acceptance from the data subject for their data to be included. One of the recommended actions from the data audit is for the organisations to be sent a consent form for completion by the data subject.
- 8.5. The information on local businesses is historic (having been transferred over from the old website). The Parish Council is not required to maintain this data and one of the recommended actions from the data audit is that this data is removed from the website in its entirety.

9. Data Security

- 9.1. The Parish Council needs to take steps to ensure that the personal data which it holds (both physical and digital) is secure. This is not a change from the current situation.
- 9.2. Where external processors are used the Parish Council needs to ensure that their approach to security is satisfactory.
- 9.3. There remains further work to do to achieve compliance in this area. The Clerk will be

focussing on this area over the coming month.

10. Data Subject Access Requests

- 10.1. Under the GDPR a Data Controller is required to provide information when requested by a data subject.
- 10.2. For most requests the data must be provided free of charge, without undue delay and within one month. The Regulations contain provisions for how to deal with complex, unfounded or excessive requests.
- 10.3. In order to ensure compliance with the requirements for dealing with a data subject access requests, the Parish Council is recommended to adopt a Data Subject Access Request Policy – draft attached at Appendix 3.
- 10.4. The Clerk has also obtained and tailored a Subject Access Request Form for internal recording purposes when/if a request is received which will support compliance with the GDPR.

11. Breach Reporting

- 11.1. A data breach is defined in the GDPR as a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclose of, or access to, personal data transmitted, stored or otherwise processed.”
- 11.2. A breach can be as simple as sending an email to the wrong recipient, or forwarding emails inappropriately (a particular risk where there is a long email string which contains personal data which may be overlooked) or can be as sophisticated as a third party “hacking” into the Parish Council website.
- 11.3. Under the GDPR a data breach must be reported to the ICO within 72 hours (including non-working days, weekends and bank holidays) unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- 11.4. The ICO will then be looking to the organisation to assess how the breach occurred and to take steps to reduce the risks of similar breaches in the future.
- 11.5. In order to ensure compliance with the requirements for dealing with a breach the Parish Council is recommended to adopt a Breach Reporting Policy – a draft is attached at Appendix 4.

12. Work Remaining

- 12.1. Further policies remaining to be prepared, reviewed and adopted:
 - Document Retention and Destruction Policy;
 - Data Security Policy;
 - Privacy Notice for Employees and Councillors. The Clerk will aim to prepare these for the May meeting.
- 12.2. Review of use of external processors, examination of the contract that exists between them and the Parish Council, consideration of how this complies with the GDPR.

13. Recommendations

- 13.1. Review of steps taken outlined in this report and identification of any further compliance work that needs to be completed which is not included in this report.
- 13.2. Decisions made on recommendations from data audit, outlined in section 5.

- 13.3. Review of the three policies/procedures attached as Appendices 2 to 4; identification of amendments required, with policies to be reconsidered at May meeting.

Appendix 1

Aston, Cote, Shifford & Chimney Parish Council

**General Data Protection Regulations
Consent to hold and publish Contact Information**

Your personal data, including your telephone number and/or your email address has previously been supplied to Aston, Cote, Shifford & Chimney Parish Council (the Parish Council) by

_____ (name of organisation)

for the purposes of inclusion on the Parish Council website (www.AstonOxon.com) so that people can contact you as a representative of that organisation. As such your personal data is in the public domain.

New Data Protection Regulations come into force on 25 May 2018 and the Parish Council is now seeking to ensure that we have a record of your informed consent for your personal details to be included on the website.

Please review and complete the form below, returning a printed, signed copy to:

Mrs Helen Sandhu, Parish Clerk
1 Manor Close
Aston
Bampton
OX18 2DD

We would be grateful if you could return the form by 30 April 2018. If we do not hear from you before that date then your details will be removed from the website. If you have any queries please contact the Clerk by email on astonpc@live.co.uk.

Consent Form

I agree that Aston, Cote, Shifford & Chimney Parish Council can keep my contact information data and include it on the AstonOxon.com website for an undisclosed time or until I request its removal.

I have the right to request modification on the information that you keep on record.

I have the right to withdraw my consent and request that my details are removed from the website and your database.

Name	
Date of birth if under 18	
Parental/Guardian Consent for any data processing activity if under 18	
Address	
Signature	
Date	

Appendix 2

Aston, Cote, Shifford & Chimney Parish Council

Privacy Notice

This Notice sets out the type of information Aston, Cote, Shifford & Chimney Parish Council collects (or are supplied with). It tells you how the information is held, who we share it with and how it is used. There are contact details for queries about your personal information. All personal data collected (or supplied) will be treated in accordance with current data protection laws in the UK.

The data controller for all information covered by this Privacy Notice is Aston, Cote, Shifford & Chimney Parish Council.

What information do we collect and what information are we supplied with?

When you contact us, we create a record in your name. To that record we add information that you give us. We keep records when you contact us. We collect and use information about our councillors and our employees. We are supplied with a copy of the register of electors by the district council. We are supplied with a copy of planning applications in our parish by the district council.

How do we use your information?

We use your personal information in the following ways:

- To process and respond to enquiries;
- To include contact details for local organisations on the parish website

Who might we share your information with?

We might share information with the district or county council or with the emergency services where we consider this would be necessary or helpful. We would seek your explicit consent to this other than where such sharing is considered necessary in an emergency or for health and safety reasons.

If you contact us your letter and/or email will be in the public domain unless you make it clear you do not wish it to be and we are able to justify confidentiality under the relevant legislation (this is very unlikely to be the case in planning matters).

Your information may be used to detect and prevent fraud in respect of public funding and we may release information to the police and other law enforcement organisations for crime prevention and detection purposes if required to do so.

We do not sell personal information to other organisations.

Automated Decision Making and Profiling

We do not use any form of automated decision making or the profiling of individual personal data.

Children

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Transfer of data outside the European Economic Area (EEA)

We will only transfer your personal information outside the EEA where necessary safeguards have been secured by contract.

How long do we keep data?

We only keep data for as long as necessary and in accordance with our Data Retention Policy, a copy of which is available on our website or from the Clerk via the contact details below.

We public on our website any changes we make to our data protection/information management policies and will notify you by other communication channels where appropriate.

Where you exercise your right to removal of your personal data, we will continue to maintain a core set of personal data (name, address and email address) to ensure that we do not contact you inadvertently in the future.

How can I access the information you hold about me?

You are entitled to know what personal information Aston, Cote, Shifford & Chimney Parish Council holds about you and how that information is processed. You are entitled to ask for your personal data to be corrected where you believe it is inaccurate. You are entitled to withdraw your consent to the processing of your personal data by the council. You are entitled to ask for your personal data to be deleted.

However, if the processing is necessary to provide you with the service (or information) you have requested then withdrawal may mean you will not receive that service or information. We may also have a lawful reason why we need to continue processing your data. We will make it clear if this is the case and discuss your concerns directly with you before we stop processing your data.

Please make any requests or complaints to:

The Data Protection Officer: Mrs Helen Sandhu
Aston, Cote, Shifford & Chimney Parish Council
1 Manor Close, Aston, Bampton, OX18 2DD
Email - astonpc@live.co.uk
Telephone – 01993 851774

If you are dissatisfied with the handling of your request or complaint, you have a right to appeal to the Information Commissioner. There is no charge for making an appeal. The contact details are:

The Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Email – casework@ico.gov.uk
Telephone – 01625 545745 or 0303 123 1113 (local rate)

Appendix 3

Aston, Cote, Shifford & Chimney Parish Council

Data Subject Access Requests

You are entitled to know what personal information Aston, Cote, Shifford & Chimney Parish Council holds about you and how that information is processed. Aston, Cote, Shifford & Chimney Parish Council is the Data Controller for all data covered by this policy.

How to make a Data Access Request

In order for us to properly understand your request you need to make it in writing, either by email or in the form of a letter.

Emails should be sent to astonpc@live.co.uk.

Letters should be sent to: Mrs Helen Sandhu, Clerk
Aston, Cote, Shifford & Chimney Parish Council
1 Manor Close, Aston, Bampton, OX18 2DD

What we do when we receive a request

It is important that we only disclose personal data to the correct person. When you submit a request we will first check that we have enough information to be sure of your identity. Often we will have no reason be uncertain, for example, if we have regularly corresponded with you. However, if we have good cause to be uncertain of your identity we can ask you to provide any evidence we reasonably need to confirm your identity. For example, we may ask you for a piece of information held in your records that we would expect you to know, a witnessed copy of your signature or proof of your address.

If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If you have been appointed to act for someone under the Mental Capacity Act 2005, you must confirm your capacity to act their behalf and explain how you are entitled to access their information. If you are the parent/guardian of a child under 13, we will need to consider whether the child can provide their consent to you acting on their behalf.

Should you make a data subject access request but you are not the data subject, you must stipulate the basis under the Data Protection Act that you consider makes you entitled to the information.

Where the records containing your personal information also contain personal information about a third party, this will be removed from any information provided unless that person has agreed to it being included.

Fees

Information you have requested will be provided free of charge unless the request is considered to be “manifestly unfounded or excessive” (see further information below), in which case a reasonable fee may be charged. A reasonable fee may be charged for supplying further copies of the same information that you have previously been supplied with. Any fee charged will be based on the actual administrative cost of providing the information.

When can you expect a response?

We will aim to provide you with the information you have requested as soon as possible and at the latest within one month of the receipt of the request. This timescale can be extended by up to three months if the information requested is complex or numerous, and in this case you will be told within one month how much extra time is required and why.

How will I receive the response?

If you have submitted your request electronically, we will respond electronically wherever possible, unless you advise us that you wish to receive the response by another means. If you have submitted your request as a printed letter, we will respond in writing to the address provided.

Your rights in relation to your data

You are entitled to ask for your personal data to be corrected where you believe it is inaccurate. You are entitled to withdraw your consent to the processing of your personal data by the council. You are entitled to ask for your personal data to be deleted.

However, if the processing is necessary to provide you with the service (or information) you have requested then withdrawal may mean you will not receive that service or information. We may also have a lawful reason why we need to continue processing your data. We will make it clear if this is the case and discuss your concerns directly with you before we stop processing your data.

Subject access requests which are “manifestly unfounded or excessive”

If we consider your request to be “manifestly unfounded or excessive”, we can charge a reasonable fee or refuse to provide the information requested. We will only apply this provision in exceptional circumstances and if we think it is applicable we will inform you within one month of the date of the request why we believe your request to be unfounded or excessive. You will have the right to complain to the Information Commissioner's Office and/or to apply to the courts to force disclosure and for compensation.

Complaints

Complaints about the way your request has been handled should be addressed to:

The Data Protection Officer: Mrs Helen Sandhu
Aston, Cote, Shifford & Chimney Parish Council
1 Manor Close, Aston, Bampton, OX18 2DD
Email - astonpc@live.co.uk
Telephone – 01993 851774

If you are dissatisfied with the handling of your request or complaint, you have a right to appeal to the Information Commissioner. There is no charge for making an appeal. The contact details are:

The Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Email – casework@ico.gov.uk
Telephone – 01625 545745 or 0303 123 1113 (local rate)

Appendix 4

Aston, Cote, Shifford & Chimney Parish Council

Data Breach Policy and Procedure

Aston, Cote, Shifford & Chimney Parish Council is a Data Controller. The Parish Council is required to keep the personal data it holds secure, to identify when a breach has occurred and to know how to deal with a breach should one occur.

The Data Protection Officer is Mrs Helen Sandhu.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

What to do when a breach occurs

The Data Protection Officer must be notified as soon as an officer or councillor becomes aware that it has occurred. This includes evenings, weekends, and holidays.

The Data Protection Officer will obtain as much information as possible from the person reporting the breach.

The Data Protection Officer will establish the likelihood and severity of the risk to people's rights and freedoms, referring to the guidance published by the Information Commissioner's Office. If it is likely that there will be risk, the Data Protection Officer will notify the Information Commissioner's Office via their website without undue delay and certainly within 72 hours of the time that the officer or councillor became aware that the breach occurred.

If the Data Protection Officer concludes that there is unlikely to be a risk to people's rights and freedoms, then the breach will not be reported. The Data Protection Officer will make a clear record of the reasons for not reporting the breach.

The Data Protection Officer will ensure that any and all steps are immediately taken to contain the breach and minimise the potential risk of harm to the people whose data has been breached.

If the Data Protection Officer concludes that the breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Protection Officer will consider whether the individuals affected should be informed directly, applying the assessment guidance published by the Information Commissioner's Office. Where necessary the Data Protection Officer will ensure that these individuals are informed directly and without undue delay to enable them to take steps to protect themselves from the potential effects of the breach.

The Data Protection Officer will also consider whether it would be appropriate to notify third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

When assessing how to deal with a breach the Data Protection Officer will ensure that the decision-making process is fully documented in accordance with the principle of accountability in data processing.

The Data Protection Officer will then carry out an investigation to determine how the breach occurred, whether any Council policies were breached and by whom, and what measures can be put in place to reduce the risk of a similar breach occurring in the future.

If the breach is deemed to be due to any action or inaction by a councillor or officer, then there will be an assessment of whether it will be appropriate to invoke the Parish Council's Disciplinary Policy (for staff) or the Code of Conduct Policy (for councillors).

The role of external Data Processors

The Parish Council uses the following external organisations to store personal data:

- Dropbox to store the Parish Councils computerised documents;
- HMRC to store the Parish Council's payroll data;
- Unity Trust Bank and Santander Bank for payment processing

If an external processor suffers a breach, it is required to inform the Parish Council without undue delay as soon as it becomes aware. This requirement enables the Parish Council to take steps to address the breach and meet its reporting obligations under the GDPR.

Record Keeping

A record of all breaches will be maintained. The record will include the facts relating to the breach, its effects, the reasons why the breach was/was not reported to the Information Commissioner's Office and/or the individuals affected, and the remedial action taken.

Financial Matters**1. Cash Balances**

	£
<i>SANTANDER CURRENT ACCOUNT</i>	
Balance at 28 February 2018	NIL
Transactions in month	NIL
Balance at 31 March 2018	<u>NIL</u>
 <i>UNITY TRUST CURRENT ACCOUNT</i>	
Balance at 28 February 2018	17,657.28
March payments	(2,110.31)
VAT Refund to 31 January 2018	1,053.72
Balance at 31 March 2018	<u>16,600.69</u>
 <i>NATIONWIDE DEPOSIT ACCOUNT</i>	
Balance at 28 February 2018	39,106.79
Transactions in month	NIL
Balance at 31 March	<u>£39,106.79</u>
 <i>SANTANDER BUSINESS DEPOSIT ACCOUNT</i>	
Balance at 28 February 2018	535.59
Transactions in month: interest received	0.12
Balance at 31 March 2018	<u>535.71</u>
 TOTAL CASH HOLDING AT 31 MARCH 2018	 <u>£56,243.19</u>