Aldenham Parish Council

Data Protection Policy

March 2024~~3~~

Contents

REVISION 1	**ADOPTED OCTOBER 2020**
REVISION 2	**MARCH 2024**

1. Introduction

1.1 Aldenham Parish Council (APC) collects and uses certain types of personal information about staff, councillors, residents and other individuals who come into contact with APC. APC may be required by law to collect and use certain types of information to comply with statutory obligations related to employment and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and other related legislation.

GDPR applies to all computerised data and manual files if they come within the definition of a filing system.

2. Background

2.1 The General Data Protection Regulation (GDPR and the Data Protection Act 2018 govern the handling of personal information that identifies individuals directly or indirectly and covers both manual and computerised information. It provides aa mechanism by which individuals about whom data is held (the 'data subject') can have a certain amount of control over the way in which it is handled.

2.2 Some of the main features of the Act are:

- All data covered by the Act must be handled in accordance with the Six Data Protection Principles (see appendix a)

- The person about whom the information is held (the Data Subject) has various rights under the Act including the right to be informed about what personal data is being processed, the right to request access to that information, the right to request that inaccuracies or incomplete data are rectified, and the right to have personal data erased and to prevent or restrict processing in specific circumstances. Individuals also have the right to object to processing based on the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling); and processing of scientific/historical research and statistics. There are also rights concerning automated decision making (including profiling) and data portability.

- Processing of special catergories of data must be done under a lawful basis. This data includes information about
- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual's sex life or sexual orientation;
- genetic or biometric data for the purpose of uniquely identifying a natural person.
-
- The Data Protection Act deals with criminal offence data in a similar way to the special category data, and sets out specific conditions providing lawful authority for processing it.

- There is a principle of accountability of data controllers to implement appropriate technical and organisational measures that include internal data protection policies and procedures, staff training and awareness or the requirements of the Act, appointing a data protection officer and implementing measures that meet the principles of protection by design and default.

-

2.3

~~Personal Data~~

~~'Personal data' is defined as information that identifies an individual. A sub-set of personal data is known as 'personal sensitive data'. This special category data is information that relates to a person's:~~

- ~~race or ethnic origin;~~
- ~~political opinions;~~
- ~~religious or philosophical beliefs;~~
- ~~trade union membership;~~
- ~~physical or mental health;~~
- ~~an individual's sex life or sexual orientation;~~
- ~~genetic or biometric data for the purpose of uniquely identifying a natural person.~~

~~Personal sensitive data is given special protection, and additional safeguards apply if this information is to be collected and used.~~

~~APC does not intend to seek or hold sensitive personal data about staff or clients except where it has been notified of the information, or it comes to light via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice.~~

~~The Data Protection Principles~~

~~Article 5 of the GDPR sets out six data protection principles which must be followed at all times:~~

~~1) Personal data shall be processed fairly, lawfully and in a transparent manner;~~
~~2) Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;~~
~~3) Personal data shall be adequate, relevant and limited to what is necessary for the purpose(s) for which it is being processed;~~
~~4) Personal data shall be accurate and, where necessary, kept up to date;~~
~~5) Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;~~

3. Policy Statement

APC is committed to ensuring that personal information is handled in a secure and confidential manner in accordance with its obligations under the Data Protection Act 2018 and GDPR. APC will use all appropriate and necessary means at its disposal to comply with the Data Protection Act and associated guidance.

4Roles and Responsibilities

4.1 Data Protection Officer

The Data Protection Officer is the Council Manager and they are responsible for

- Informing APC, any data controller and any employee of APC who carries out the processing of personal data, of that persons obligations under the legislation.

- Co-Operating with the Information Commisioners Office (ICO), acting as the contact for the ICO, and monitoring the policies of APC that relate to personal data.

4.2 Aldenham Parish Council (APC)

APC will be responsible for ensuring that it complies with its responsibilities under any Data Protection Act and related regulations through monitoring of activities and incidents reported by the Data Protection Officer. APC will also ensure that there are sufficient resources supplied to ensure compliance with the Data Protection Act.

4.3 All Staff and Councillors

All staff and councillors will ensure that

- Personal information is treated in a confidential manner in accordance with this and any associated policies.

- The rights of data subjects are respected at all times.

- Privacy notices will be made available to inform individuals how their data is being processed.

- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose.

- Personal information is only disclosed on a strict 'need to know' basis, to recipients who are entitled to that information.

- Personal information held within applications, systems, personal or shared drives is only accessed in order to carry out work responsibilities.

- Personal information is recorded accurately and is kept up to date.

- They refer any subject access requests and/or requests in relation to the rights of individuals to the Data Protection Officer.

- They raise actual or potential breaches of the Data Protection Act to the Data Protection Officer as soon as the breach is discovered.

It is the responsibility of all staff and councillors to ensure that they comply with the requirements of this policy and any associated policies or procedures.

5. Records Management

5.1 Good records management practice plays a pivotol role in ensuring that APC is able to meet its obligations to provide information, and to retain it, in a timely and effective manner in order to meet the requirements of the Act. All records should be retained and disposed of in accordance with the APC retention schedule.

6. Consent

6.1 APC will take all reasonable steps to ensure that service users, members of staff, volunteers and contractors are informed of the reasons APC requires information from them, how that information will be used and who it will be shared with. This will enable the data subject to give explicit informed consent to APC handling their data where the legal basis for processing is consent.

6.2 Should APC wish to use personal data for any purpose other than that specified when it was originally obtained, the data subjects explicit consent should be obtained prior to using the data in the new way unless exceptionally such use is in accordance with other provisions of the Act.

7. Accuracy and Data Quality

7.1 APC will ensure that all reasonable steps are taken to confirm the validity of personal information directly with the data subject.

7.2 Where a member of the public exercises their right for their data to be erased, rectified, or restricted, or where a member of the public objects to the processing of their data, the Data Protection Officer must be notified and the appropriate procedures followed.

8 Complaints

8.1 Any expression of dissatisfaction from an applicant with reference to APC's handling of personal information will be treated as a complaint, and handled under APC's complaint process. The Data Protection Officer will be involved in responding to the complaint.

8.2 Should the complainant remain dissatisfied with the outcome of their complaint to APC, they will be informed that a complaint can be made to the information Commisioners Office who will then investigate the complaint and take action where necessary.

9. Security and Confidentiality

9.1 All staff and councillors must insure that information relating to identifiable individuals is kept secure and confidential at all times. APC will ensure that its holdings of personal data are properly secured from loss or corruption and that no unauthorised disclosures of personal data are made.

9.2 APC will ensure that information is not transferred to countries outside of the European Economic Area (EEA) unless that country has an adequate level of protection for security and confidentiality of information which has been confirmed by the Information Commissioner.

10 Rights of Data Subjects

10.1 Individuals should also make requests in writing to APC if they wish to exercise their other rights under legislation.

10.2 Individuals wishing to request their information as a subject access request should contact APC, who will arrange for the information to be processed in accordance with the Data Protection Act.

~~Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.~~

~~In addition to this, APC is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law.~~

~~APC is committed to complying with the data protection principles at all times. This means that;~~

~~APC inform individuals as to the purpose of collecting any information from them, as and when APC ask for it and will identify who we will share the information with and how long APC will retain this information.~~

~~be responsible for checking the quality and accuracy of the information;~~

~~regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;~~

~~ensure that when information is authorised for disposal it is done in accordance with our disposals policy;~~

~~ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;~~

~~share personal information with others only when it is necessary and legally appropriate to do so;~~

~~set out clear procedures for responding to requests for access to personal information known as subject access requests;~~

~~report any breaches of the GDPR.~~

Conditions for Processing

- The individual has given consent that is specific to the particular type of processing activity.
- The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.
- The processing is necessary for the performance of a legal obligation to which we are subject.
- The processing is necessary to protect the vital interests of the individual or another.

Use of Personal Data by APC

APC collects and uses certain types of personal information about staff, councillors, residents and other individuals who come into contact with the Council. In each case, the personal data must be treated in accordance with the data protection principles.

Any wish to limit or object to use of personal data should be notified to the PCM in writing. If, in the view of the PCM, the objection cannot be maintained, the individual will be given written reasons why the Council cannot comply with their request.

Staff, councillors and Volunteers

The personal data held about staff, councillors and volunteers will include contact details, employment history, information relating to career progression, information relating to DBS checks and photographs.

The data is used to comply with legal obligations placed on APC in relation to employment. APC may pass information to other regulatory authorities where appropriate. Personal data will also be used when giving references.

It should be noted that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

Other Individuals
APC may hold personal information in relation to other individuals who have contact with APC, such as volunteers and members of the Youth Council. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

Security of Personal Data
APC will take reasonable steps to ensure that members of staff and councillors will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR. APC will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

Disclosure of Personal Data to Third Parties
The following list includes the most usual reasons that APC will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee;
- For the prevention or detection of crime;
- For the assessment of any tax or duty;
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon APC (other than an obligation imposed by contract);
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- For the purpose of obtaining legal advice;

APC may receive requests from third parties to disclose personal data it holds about staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or APC.

All requests for the disclosure of personal data must be sent to the PCM, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

Subject Access Requests
Anybody who makes a request to see any personal information held about them by APC is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure.

A subject access request must be made in writing. APC may ask for any further information reasonably required to locate the information.

All requests will be handled in line with the Subject Access procedural note.

Other Rights of Individuals
Right to restrict processing

An individual has the right to object to the processing of their personal data and to block or suppress the processing.

Where such an objection is made, it must be sent to the PCM who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The PCM shall be responsible for notifying the individual of the outcome of their assessment within 20 working days of receipt of the objection.

Right to rectification
An individual has the right to request the rectification of inaccurate data or incomplete data without undue delay. Where any request for rectification is received, it should be sent to the PCM and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified within 20 days.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given details of how to appeal to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure
Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- Where consent is withdrawn and there is no other legal basis for the processing;
- Where an objection has been raised under the right to object, and there is no overriding legitimate interest for continuing the processing;
- Where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
- Where the data has to be erased in order to comply with a legal obligation.

The PCM will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to object
An individual has the right to object to:

- Processing based upon legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

- Direct marketing (including profiling);

- Processing for purposes of scientific /historical research and statistics.

Where such an objection is made, it must be sent to the PCM who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

Right to portability
If an individual want to send their personal data to another organisation they have a right to request that APC provides their information in a structured, commonly used, and machine-readable format. This right is limited to situations where APC is processing the information on the basis of consent or performance of a contract. If a request for this is made, it should be forwarded to the PCM.

Breach of any Requirements of the GDPR
Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the PCM. Once notified, the PCM shall assess:

- The extent of the breach;
- The risks to the data subjects as a consequence of the breach;
- Any security measures in place that will protect the information;
- Any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the Clerk concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of APC.

The Information Commissioners Office will be told details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- The contact point for any enquiries;
- The likely consequences of the breach;
- The measures proposed or already taken to address the breach

If the breach is likely to result in a high risk to the affected individuals then the PCM shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:
- The nature of the breach;
- Who to contact with any questions;

- The measures taken to mitigate any risks.

The PCM shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by APC and a decision made about implementation of those recommendations.

This policy was adopted by Aldenham Parish Council at its meeting of 25th October 2020 and will be reviewed when necessary.

~~THIS POLICY MUST BE COMPLIED WITH AT ALL TIMES.~~

Appendix a

The Data Protection Principles

Article 5 of the GDPR sets out six data protection principles which must be followed at all times:

6) Personal data shall be processed fairly, lawfully and in a transparent manner;
7) Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
8) Personal data shall be adequate, relevant and limited to what is necessary for the purpose(s) for which it is being processed;
9) Personal data shall be accurate and, where necessary, kept up to date;
10) Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;

Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

In addition to this, APC is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law.

APC is committed to complying with the data protection principles at all times. This means that;

APC inform individuals as to the purpose of collecting any information from them, as and when APC ask for it and will identify who we will share the information with and how long APC will retain this information.

~~be responsible for checking the quality and accuracy of the information;~~

regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;

ensure that when information is

authorised for disposal it is done in accordance with our disposals policy;

ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

share personal information with others only when it is necessary and legally appropriate to do so;

set out clear procedures for responding to requests for access to personal information known as subject access requests;

report any breaches of the GDPR.

Appendix 1

GENERAL PRIVACY NOTICE

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom

including the General Data Protection Regulation (the "GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Aldenham Parish Council which is the data controller for your data.

Other data controllers the council works with:

- Local Authorities/Town/Parish Councils
- Community groups
- Charities
- Other not for profit entities
- Contractors

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be "joint data controllers" which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.
A description of what personal data the council processes and for what purposes is set out in this Privacy Notice.

The council will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

How we use sensitive personal data

- We may process sensitive personal data including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.

  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council

- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and the council's obligations to you.

We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the acceptance of an allotment garden tenancy
Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

Sharing your personal data

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The data controllers listed above under the heading "Other data controllers the council works with";
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:
When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1) *The right to access personal data we hold on you*
   - At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
   - There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) *The right to correct and update the personal data we hold on you*
   if the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3) *The right to have your personal data erased*
   - If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
   - When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4) *The right to object to processing of your personal data or to restrict it to certain purposes only*
   - You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) *The right to data portability*
   - You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6) *The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained*
   - You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7) *The right to lodge a complaint with the Information Commissioner's Office.*
   - You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

<u>Transfer of Data Abroad</u>

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. [Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas].

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on www.aldenham-pc.gov.uk This Notice was last updated in October 2020.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:
The Data Controller, Aldenham Parish Council, First Floor, The Radlett Centre, 1 Aldenham Avenue, RADLETT, WD7 8HL
Email: manager@aldenham-pc.gov.uk

Appendix B

Privacy Policy - Youth

This policy had been created in order to comply with the new General Data Protection Regulations (GDPR) which came into force on 25th May 2018 and supersedes the existing Data Protection Act 1998.

Your personal data – what is it?

"Personal data" is any information about a living individual, which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the personal data alone or in conjunction with any other personal data. The processing of personal data is governed by legislation relating to personal data, which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR) and other local legislation relating to personal data and rights such as the Human Rights Act.

Council information

This Privacy Policy is provided to you by Aldenham Parish Council, which is the data controller for your data. The Council's address is: First Floor, The Radlett Centre, 1 Aldenham Avenue, RADLETT, WD7 8HL.

Policy

Our policy explains the reasons why we might ask for your personal data. It will cover three main areas. What data we collect from you and why; how we keep it safe and process it in accordance with the law, including who has access to it besides Aldenham Parish Council and what we are doing to protect your rights as a data subject, and how you can exercise those rights.

The Personal Data We Collect

Your personal data is collected for several reasons. These include:

- Named contacts in organisations that will enable us to deliver Radlett Youth Council & activities.
- Details of people wanting to participate in our projects
- Details of young people wishing to participate in our organised events
- Names of parents/guardians of young people, required for safeguarding purposes
- Names of those wishing to be informed of activities
- Details of people providing or contributing to our activities

Why We Hold Personal Data

Several activities require us to process personal data. These include:

- Delivering activities or programmes
- Internal record keeping
- Sending you information we believe you will find interesting, using the email address you have provided or through Social Media.

How We Keep Personal Data Secure

Aldenham Parish Council takes data security extremely seriously. We have therefore implemented appropriate digital, managerial and physical procedures to ensure your data is not lost, stolen, damaged or disclosed to any unauthorised person or organisation.

Who Sees Personal Data

The council will implement appropriate security measures to protect your personal data. This section of the Privacy Policy provides information about the third parties with whom the council will share your personal data. These third parties also have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- Suppliers, contractors, local authorities, activity providers, workplaces and schools. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.
- Advertising on social media

How We Will Uphold Your Rights as A Data Subject

We will do our best to keep the data we hold accurate. However, if you spot any errors in the data we hold on you, please let us know and we will rectify them.

Our promise to you, is to never use your personal data for anything we haven't already told you about. Unless obliged to do so by law, we won't share your data with anyone other than the organisations we have told you about. We will never use your data for any form of profiling or automated decision-making.

You can ask to see what personal data we hold on you at any time. If you gave us your consent to process your data, you can withdraw that consent. You can also request that we delete it, or tell us not to use it for some of the purposes described in this policy. Where applicable, we can provide your data to you in a portable digital format.

Your rights and your personal data

You have the following rights with respect to your personal data:
When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

- *The right to access personal data we hold on you*
- *The right to correct and update the personal data we hold on you*
- *The right to have your personal data erased*
- *The right to object to processing of your personal data or to restrict it to certain purposes only*
- *The right to data portability*
- *The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained*
- *The right to lodge a complaint with the Information Commissioner's Office.* You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Additional notes

To help us inform the community of activities in the region, we may include links from our website to the websites of other organisations. Please note that we cannot be responsible for either the contents of these websites or their data protection measures. Our privacy policy does not cover information you provide to these websites. We,

therefore, recommend you exercise caution and review the privacy policies of the sites in question before submitting your personal data to them.

Our website may collect tracking data from your computer or device. To find out more about this – including how to prevent such tracking – please see our Cookie Policy.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Policy, then we will provide you with a Privacy Notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this policy

We keep this Privacy Policy under regular review and we will place any updates on www.aldenham-pc.gov.uk

Contact Details

Please contact us if you have any questions about this Privacy Policy or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:
Aldenham Parish Council, First Floor, The Radlett Centre, 1 Aldenham Avenue, RADLETT, WD7 8HL.

Appendix C

Subject Access Policy

This policy had been created in order to comply with the new General Data Protection Regulations (GDPR) which come into force on 25th May 2018 and supersedes the existing Data Protection Act 1998.

Data subjects have the right to access personal data held on them by APC. Details are set out in the Privacy Notice on the Council's website.

This policy is in place to ensure that internal procedures on handling of Subject Access Requests (SARs) are accurate and complied with and includes:

(1) Responsibilities (who, what)
(2) Timing
(3) Changes to data
(4) Handling requests for rectification, erasure or restriction of processing.

APC will ensure that personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.

APC has implemented standards on responding to SARs.

Upon receipt of a SAR

(a) The data subject will be informed who at APC to contact, the Data Controller.
(b) The identity of the data subject will be verified and if needed, any further evidence on the identity of the data subject may be requested.
(c) The access request will be verified; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not additional information will be requested.
(d) Requests will be verified as to them being unfounded or excessive (in particular because of their repetitive character); if so, APC may refuse to act on the request or charge a reasonable fee.
(e) Receipt of the SAR will be promptly acknowledged and the data subject will be informed of any costs involved in the processing of the SAR.

(f) Whether APC processes the data requested will be verified. If APC does not process any data, the data subject will be informed accordingly. At all times the internal SAR policy will be followed and progress may be monitored.
(g) Data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned may be permitted.
(h) The data requested will be verified to establish if it involves data on other data subjects. This data will be filtered before the requested data is supplied to the data subject; if data cannot be filtered, other data subjects will be contacted to give consent to the supply of their data as part of the SAR.

Responding to a SAR

(i) APC will respond to a SAR within one month after receipt of the request:
  (i) If more time is needed to respond to complex requests, an extension of another two months is permissible, and this will be communicated to the data subject in a timely manner within the first month;
  (ii) if APC cannot provide the information requested, it will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.
(j) If a SAR is submitted in electronic form, any personal data will be preferably provided by electronic means as well.
(k) If data on the data subject is processed, APC will ensure as a minimum the following information in the SAR response:
  (i) the purposes of the processing;
  (ii) the categories of personal data concerned;
  (iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses
  (iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
  (v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
  (vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");
  (vii) if the data has not been collected from the data subject: the source of such data;
  (viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
(l) Provide a copy of the personal data undergoing processing.

Implementing the Subject Access Requests Policy – APC Checklist on what MUST be done

On receipt of a subject access request it must be **forwarded** immediately to the PCM who will **identify** whether a request has been made under the Data Protection legislation

1. A member of staff, and as appropriate, councillor, who receives a request to locate and supply personal data relating to a SAR **must** make a full exhaustive **search** of the records to which they have access.

2. All the personal data that has been requested **must** be **provided** unless an exemption applies. (This will involve a search of emails/recoverable emails, word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems.)
3. A **response must** be provided within one calendar month after accepting the request as valid.
4. Subject Access Requests **must** be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.
5. Councillors, the PCM and Assistant Manager **must** ensure that the staff they manage are **aware** of and follow this guidance.
6. APC **must** provide where necessary an explanation with the personal data in an "intelligible form", which will include giving an explanation of any codes, acronyms and complex terms. The personal data will be supplied in a permanent form except where the requestor agrees or where it is impossible or would involve undue effort. Agreement may be sought with the requestor that they will view the personal data on screen or inspect files on APC premises. Any exempt personal data will be redacted from the released documents with explanation why that personal data is being withheld.
7. APC **must** ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by APC relating to the data subject. What personal data is needed will be clarified with the requestor, who must supply their address and valid evidence to prove their identity. APC accepts the following forms of identification (* These documents must be dated in the past 12 months; +These documents must be dated in the past 3 months):
    - Current UK/EEA Passport
    - UK Photocard Driving Licence (Full or Provisional)
    - Firearms Licence / Shotgun Certificate
    - EEA National Identity Card
    - Full UK Paper Driving Licence
    - State Benefits Entitlement Document*
    - State Pension Entitlement Document*
    - HMRC Tax Credit Document*
    - Local Authority Benefit Document*
    - State/Local Authority Educational Grant Document*
    - HMRC Tax Notification Document
    - Disabled Driver's Pass
    - Financial Statement issued by bank, building society or credit card company+
    - Judiciary Document such as a Notice of Hearing, Summons or Court Order
    - Utility bill for supply of gas, electric, water or telephone landline+
    - Most recent Mortgage Statement
    - Most recent council Tax Bill/Demand or Statement
    - Tenancy Agreement
    - Building Society Passbook which shows a transaction in the last 3 months and your address

8. Where a requestor is not satisfied with a response to a SAR, APC **must** manage this as a **complaint** under the APC Complaints Policy.