HEVER PARISH COUNCIL – GDPR POLICY 2022

General Data Protection Regulation (GDPR) 2018.

Introduction

Hever Parish Council (HPC) controls and processes very little personal information (and rarely sensitive information) and has always respected privacy. HPC does not use data for marketing or business purposes.

HPC *for the purposes of data protection* is NOT classed as a public authority as will not normally process personal data on a "large scale".

The GDPR enhances the existing data protection legislation (Data Protection Act 2018). It is not a legal requirement to appoint a Data Protection Officer (DPO). The Clerk may fulfil the function of a Data Protection Compliance Officer.

The following actions have been taken by HPC since 2018;

1. Registered and fee paid with the Information Commissioners Office ICO (£40 / year)
2. National Association of Local Councils (NALC) toolkit (08/2018) completed (October 2018, April 2020) and will be undertaken annually.
3. Data audit questionnaire and internal register of processing activities (NALC) completed (October 2018, April 2020) and will be undertaken annually. See HPC April 2020 personal data record & register of processing activities document (Register to be completed by April 2021).
4. All Councillors and Clerk now have HPC email address (@hever.org) set up by independent IT company and do not use private email addresses for Council work.
5. Use of private devices to be reviewed by April 2023.
6. Updated website (hever.org) and contains privacy notice. http://hever.org/?s=PRIVACY+NOTICE and information re; cookies etc.
7. Personal information is stored in a locked filing cabinet / safe.
8. Data protection and privacy policy (Appendix 1) and notice (Ap. 2 & 3) shared and all those currently on mailchimp general contact list contacted.
9. Clearer and easier to opt out of all communications.
10. Councillor training and GDPR on every full Council meeting agenda.
11. New personal computer for the Clerk purchased and installed by HPC with full encryption (Windows 10 pro version).
12. Data Privacy Impact checklist completed – no assessment (DPIA) required as currently no new technologies used for high risk data processing activities.
13. Two privacy notices (ones for "general" (Ap. 2) and another for "staff / contractors etc. (Ap. 3) completed
14. Data subject access policy and template response (Ap. 4)
15. Data security breach process (Ap. 5)

NB. HPC do not store or process "special categories of personal data" or hold data relating to children.

Further information;
https://www.kentalc.gov.uk/GDPR_22945.aspx
https://www.nalc.gov.uk/news/entry/959-nalc-launches-new-toolkit-on
https://ico.org.uk/for-organisations/

Appendix 1. Data protection and privacy policy

1. 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.

2. Council information

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

(a) Personal data may be collected from hever.org

3. Who are the data controllers?

(a) Hever Parish Council

(b) Other local authorities

(c) Community groups

(d) Charities

(e) Other not for profit entities

(f) Contractors

4. What personal is collected?

- 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 demographic information such as gender, age, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The data we process may include sensitive personal data or other special categories of data such as 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 sex life or sexual orientation.

- Website data - e.g.
  - Information from synching with other software or services
  - Interaction with social media
  - Information about payments
  - Access to social media profiles
  - Demographic information
- Information collected automatically from use of the service
  - Device information
  - Log information (including IP address)
  - Location information (how is location collected/inferred)
  - Device sensor information
  - Site visited before arriving
  - Browser type and or OS
  - Interaction with email messages
- Information from other sources e.g.
  - Referral or recommendation programmes
  - Publicly accessible sources
- Information from cookies or similar technologies (incl. in-app codes) (including whether session or persistent) e.g.
  - Essential login/authentication or navigation
  - Functionality – remember settings
  - Performance & Analytics – user behaviour
  - Advertising/retargeting

  - Any third party software served on users
  - Other
- Nature of any outbound communications with website users
  - Email
  - Telephone (voice)
  - Telephone (text)

5. 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.

6. 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 notify you of changes to our facilities, services, events and staff, councillors and role holders;
- 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.

7. What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and duties. 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. Sometime 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 Policy sets out your rights and the council's obligations to you in detail.

We may also 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 use of sports facilities, or 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.

8. Sharing your 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):

- 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 facilities or events for the community.

9. 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 current 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.

10. 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.

(i) The right to access personal data we hold on you
(ii) The right to correct and update the personal data we hold on you
(iii) The right to have your personal data erased
(iv) The right to object to processing of your personal data or to restrict it to certain purposes only
(v) The right to data portability
(vi) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained
(vii) 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.

11. Transfer of Data Abroad

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].

12. 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.

13. Changes to this policy

We keep this Privacy Policy under regular review and we will place any updates on hever.org This Policy was last updated in October 2018.

14. 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:

The Data Controller, Hever Parish Council
Email: clerk@hever.org

Appendix 2. GENERAL PRIVACY NOTICE

1a. is to be used for residents and members of the general public (but not for staff, councillors or anyone with a role in the local council). 1b. is for staff members, councillors and anyone else with a role in the council.]

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 list 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 Hever Parish Council which is the data controller for your data.

Other data controllers the council works with:

- other data controllers, such as local authorities
- 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;
- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- 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 notify you of changes to our facilities, services, events and staff, councillors and other role holders;
- 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 use of sports facilities, or 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 facilities or 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.

Transfer of Data Abroad

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.hever.org. This Notice was last updated in October 2021.

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, Hever Parish Council

Email: clerk@hever.org

Appendix 3. Privacy Notice

1b. is to be used for staff members, councillors and anyone else with a role in the council (but not for residents and members of the general public.

For staff*, councillors and Role Holders**

*"Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis

**Includes, volunteers, contractors, agents, and other role holders within the council including former staff*and former councillors. This also includes applicants or candidates for any of these roles.

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, photograph, video, 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 list 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 Hever Parish Council which is the data controller for your data.

The council works together with:

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be "joint data controllers". This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration, then the data controllers will be independent and will be individually responsible to you.

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.

What data do we process?

- Names, titles, and aliases, photographs.
- Start date / leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.

- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about your use of our information and communications systems.

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

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records;
- To seek your views or comments;
- To process a job application;
- To administer councillors' interests
- To provide a reference.

Our processing may also include the use of CCTV systems for monitoring purposes.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].

How we use sensitive personal data

- We may process sensitive personal data relating to staff, councillors and role holders 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, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- 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?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- 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.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary 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.
- [We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.] [Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.]

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions , or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies
- Professional advisors
- Trade unions or employee representatives

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 responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with 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 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.

Transfer of Data Abroad

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, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on www.hever.org This Notice was last updated in October 2018.

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, Hever Parish Council

Email: clerk@hever.org

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.

HEVER PARISH COUNCIL

Appendix 4. Subject access policy and template response letters.

Subject Access Requests ("SAR") Checklist

A. Inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted (e.g. a dedicated email address).

B. Make sure a SAR policy is in place within the council and that internal procedures on handling of SARs are accurate and complied with. Include, among other elements, provisions on:

(1) Responsibilities (who, what)

(2) Timing

(3) Changes to data

(4) Handling requests for rectification, erasure or restriction of processing.

C. Ensure 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.

D. Where possible, implement standards to respond to SARs, including a standard response.

1. Upon receipt of a SAR

(a) Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.

(b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.

(c) Verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.

(d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, you may refuse to act on the request or charge a reasonable fee.

(e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

(f) Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.

(g) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.

(h) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

2. Responding to a SAR

(a) 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, provided this is communicated to the data subject in a timely manner within the first month;

(ii) if the council cannot provide the information requested, it should, inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

(c) If data on the data subject is processed, make sure to include 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[1] or EU model clauses[2];

(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.

(d) Provide a copy of the personal data undergoing processing.

[1] "Binding Corporate Rules" is a global data protection policy covering the international transfer pf personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisations head quarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

[2] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

Sample Subject Access Requests Policy

What must I do?

1. ***MUST***: On receipt of a subject access request you must **forward** it immediately to the Clerk.

2. ***MUST***: We must correctly **identify** whether a request has been made under the Data Protection legislation

3. ***MUST***: 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.

4. ***MUST***: All the personal data that has been requested must be **provided** unless an exemption can be applied.

5. ***MUST***: We must **respond** within one calendar month after accepting the request as valid.

6. ***MUST***: Subject Access Requests must be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.

7. ***MUST***: Councillors and managers must ensure that the staff they manage are **aware** of and follow this guidance.

8. ***MUST***: Where a requestor is not satisfied with a response to a SAR, the council must manage this as a **complaint**.

How must I do it?

1. Notify the Clerk upon receipt of a request.
2. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. You should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity. The council 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
3. Depending on the degree to which personal data is organised and structured, you will need to search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.

4. You must not withhold personal data because you believe it will be misunderstood; instead, you should provide an explanation with the personal data. You must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. You must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

5. Make this clear on forms and on the council website

6. You should do this through the use of induction, my performance and training, as well as through establishing and maintaining appropriate day to day working practices.

7. A database is maintained allowing the council to report on the volume of requests and compliance against the statutory timescale.

8. When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

E. **Sample letters**

3. All letters must include the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) 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[3] or EU model clauses[4];

(d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) 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;

(f) the right to lodge a complaint with the Information Commissioners Office ("ICO");

(g) if the data has not been collected from the data subject: the source of such data;

(h) 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.

4. Replying to a subject access request providing the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data you requested.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

5. Release of part of the personal data, when the remainder is covered by an exemption

"[Name] [Address]

[Date]

Dear [Name of data subject]

[3] "Binding Corporate Rules" is a global data protection policy covering the international transfer pf personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisations head quarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

[4] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

6. Replying to a subject access request explaining why you cannot provide any of the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*.

I regret that we cannot provide the personal data you requested. This is because *[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Your data protection officer will be able to advise if a relevant exemption applies and if the council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the council should set out the reason why some of the data has been excluded.]

Yours sincerely"

HEVER PARISH COUNCIL

Appendix 5. Data security breach process

Part A: Checklist of what to include in a security incident response policy.

1.1 A. A data breach of any size is a crisis management situation, which could put an entire council at risk. Data security is not an IT issue, it is an organisational risk, and breach response should involve people from a number of roles across the council.

1.2 B. Planning for a breach is therefore essential; every council should have in place a breach response plan, and should designate, in advance, a breach response team which can be convened at short notice to deal with the crisis.

1.3 C. Understanding the issues that arise in a breach situation, and practising managing a breach, are essential to effective breach response. Failure to plan and practise increases the regulatory, litigation and reputation risk to the entire council.

1.4 D. The checklist below sets out the key issues which a council should consider in preparing for a data breach.

1.5 1. The breach response plan

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

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

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

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

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

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

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

1.13 (h) Have you tested your breach response plan?

1.14 2. Legal issues

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

1.16 (b) Can you pause document destruction processes?

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

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

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

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

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

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

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

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

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

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

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

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

1.29 3. Forensic IT

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

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

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

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

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

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

1.36 4. Cyber breach insurance

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

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

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

1.40 5. Data

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

1.42 (b) Is your data appropriately classified?

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

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

1.45 (e) Do you have appropriate regression checks to ensure you are storing only the data you should be?

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

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

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

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

1.50 6. Data subjects

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

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

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

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

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

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

1.57 7. Public Relations ("PR")

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

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

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

Part B: Cybersecurity checklist

1.61 A. Data security is an ever-increasing risk for most organisations including councils. However, the number of breaches which are the result of highly sophisticated attacks from hackers is still very limited; most breaches are still the result of human error or relatively unsophisticated phishing attacks.

1.62 B. Many of the steps that councils can take to limit the risk and impact of a personal data breach are relatively simple to implement, but require effective policies and controls to implement. Good information security crosses over a number of policies – it is not just a matter of putting in place an information security policy. The checklist below sets out the key issues that a council should deal with, and which should be implemented where appropriate across the entire suite of internal policies.

1.63 1. Glossary

1.64 (a) "Acceptable use policy" or fair use policy, is a set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.

1.65 (b) "Bring Your Own Device" ("BYOD") policy is useful where staff are permitted to use their own tablets, mobile devices and other IT equipment and deals with appropriate security measures that they should comply with.

1.66 (c) "Cyber security" is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

1.67 (d) "Firewall" is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

1.68 (e) "Multifactor authentication" is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction for example using a password and a separate delivered pin number (sometimes described as "2 step" authentication).

1.69 (f) "Network security policy" is a generic document that outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of the security/ network security environment.

1.70 (g) "Penetration testing" (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

1.71 (h) "Remote access policy" is a document which outlines and defines acceptable methods of remotely connecting to the internal network.

1.72 (i) "Remote access" is the ability to get access to a computer or a network from a remote distance.

1.73 (j) "Wifi" a facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

1.74 2. Do you have appropriate policies in place?

1.75 (a) Information security policy

1.76 (b) Privacy policy

1.77 (c) "Bring Your Own Device" ("BYOD")policy

1.78 (d) Remote access policy

1.79 (e) Network security policy

1.80 (f) Acceptable use/internet access policy

1.81 (g) Email and communication policy

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

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

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

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

1.86 (d) Do you ensure physical security of premises?

1.87 (e) Do you allocate sufficient budget to cyber security?

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

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

1.90 (h) Do you have appropriate cyber breach insurance in place?

1.91 4. People

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

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

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

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

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

1.97 (f) Do staff and councillors understand the risks of using public wifi?

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

1.99 5. Hardware, data, encryption and technology

1.100 (a) Is backup personal data encrypted?

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

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

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

1.104 (e) Are your wireless networks appropriately secured?

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

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

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

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

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

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

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

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

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

1.114 6. Third parties

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

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

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

1.118 (d) Do you build appropriate contractual obligations on third parties to take steps to keep data secure?

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

1.120 7. Remote access/BYOD

1.121 (a) Do you require multifactor authentication where appropriate?

1.122 (b) Do you allow remote access?

1.123 (c) If so, do you have appropriate software and controls in place to ensure it is secure?

1.124 (d) Do you have appropriate policies to secure mobile devices?

1.125 (e) Is data encrypted on mobile devices?

1.126 (f) Can mobile devices be remotely wiped?

1.127 (g) If you use BYOD, do you apply appropriate restrictions to personal use to maintain security?

1.128 8. User accounts / passwords

1.129 (a) Do you require unique user accounts?

1.130 (b) Do you require multifactor authentication where appropriate?

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

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

(e) Do you automatically prevent use of common passwords?

Glossary: The jargon explained:

Consent is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.

Data controller is the person or organisation who determines the how and what of data processing.

Data processor is the person or firm that processes the data on behalf of the controller.

Data subject is the person about whom personal data is processed.

Personal data is information about a living individual which is capable of identifying that individual. E.g. a name, email addresses, photos.

Privacy Notice is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

Processing is anything done with/to personal data (obtaining, recording, adapting or holding/storing) personal data.

Sensitive personal data is also described in the GDPR as 'special categories of data' and is the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.

National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk

109 Great Russell Street
London WC1B 3LD