CHOLSEY PARISH COUNCIL

To all members of the Council, you are hereby summoned to attend the meeting of Cholsey Parish Council on Wednesday 17th April 2024 at 7.15pm to be held at The Pavilion, Station Road, Cholsey for the purpose of transacting the following business.

11th April 2024
Claire Bird, Clerk to the Council

1. **To co-opt new members to the Parish Council**

2. **To receive apologies for absence**

3. **To receive Declarations of Personal and Pecuniary Interest for any agenda items**

4. **To hear questions or comments from members of the public (max 15 mins)**

5. **To approve and sign the minutes of the meeting held on 13th March 2024 (Appendix A)**

6. **To receive any reports from County and/or District Councillor**

7. **To note the Clerk's Update, in particular:**
    a. **To approve and adopt the following:**
        i. **Health and Safety Policy (Appendix B)**
        ii. **GDPR Data Protection Policy and GDPR Data Breach Policy (Appendix C and Appendix D)**
    b. **Annual Community Meeting planning update**

8. **To note the Estate Manager's Report (Appendix E), in particular:**
    a. **To agree next steps in the Tree Risk Management process**
    b. **To agree next steps in the Car Park Renovation project**

9. **To agree next steps in the Recreation Ground Path project**

10. **To receive update on developing a Community Emergency Plan**

11. **To receive update from the Transport Lead (Cllr Collins), in particular:**
    a. **To agree Station Working Group Terms of Reference (Appendix F)**
    b. **To appoint members to serve on the Station Working Group**

12. **Finance**
    a. **To agree response to 2024/2025 S137 grant request for 'Fun in the Park'**
    b. **To approve payments made and note payments received (Appendix G)**

13. **To agree responses to planning applications as at 11th April 2024 – none received since previous agenda**

14. **To note planning decisions as at 11th April 2024 – none received since previous agenda**

15. **Items for information or inclusion on future agenda**

CHOLSEY PARISH COUNCIL

APPENDIX A

Minutes of the meeting of Cholsey Parish Council duly convened and held on Wednesday 13th March 2024 at 7.15pm at The Great Hall, Cholsey Meadows

Present were Cllr V. Bolt, Cllr J. Finch, Cllr G. Herbert, Cllr J. Hope-Smith, Cllr L. Nixon (Chair), Cllr M. Smith

Also present were C. Bird (Clerk), V. Beardall-Richards (Environment Coordinator), one member of public

Start time: 7.15pm
End time: 9.10pm

187. To receive apologies for absence
Apologies were accepted from Cllr D. Bamford, Cllr J. Collins, Cllr P. Jenkins and Cllr K. Ofield.

188. To receive Declarations of Personal and Pecuniary Interest for any agenda items
There were none.

189. To hear questions or comments from members of the public (max 15 mins)
There were none.

190. To approve and sign the minutes of the meeting held on 21st February 2024
It was **resolved** to approve the minutes of the meeting held on 21st February and they were signed by Cllr Nixon.

191. To receive any reports from County and/or District Councillor
There were none.

192. To note the Clerk's Update, in particular:

a. To approve and adopt the following draft policies:

i. Biodiversity policy

The new Biodiversity policy was approved and the Clerk will publish this on the Council web site. The logistics involved in carrying out a biodiversity audit of Council managed land will be explored further. It is hoped that the community might help in this. The next step required by the Biodiversity Duty (*Environment Act 2021*) is to develop a biodiversity action plan of specific objectives.

ii. Health and Safety policy

Cllr Nixon asked that the Reporting of Accidents section be revised to make sure the scope is clear. The Clerk will bring a revised version to the next meeting.

b. To discuss and approve request received to hold a Family Fun day on the Recreation Ground on 22nd June 2024

Cllr Bolt has been informed that the proposed event has been postponed for now.

c. Annual Community Meeting planning update

Plans are underway for Saturday 11th May. The Clerk is contacting community groups to invite them to participate and will advertise the date via posters, social media, web site. Councillors were reminded of the date for their diaries and a small Council working party will be formed to organise the event.

d. To approve full Council meeting dates for the remainder of 2024

The following full Council meeting dates were confirmed:

Wednesday 17th April 2024, 7.15pm, The Pavilion

Wednesday 8th May 2024, 7.15pm, The Pavilion

Wednesday 5th June 2024, 7.15pm, The Pavilion

Wednesday 26th June 2024, 7.15pm, The Great Hall

Wednesday 17th July 2024, 7.15pm, The Pavilion

Wednesday 18th September 2024, 7.15pm, The Pavilion

Wednesday 16th October 2024, 7.15pm, The Pavilion

Wednesday 20th November 2024, 7.15pm, The Great Hall? (tbc)

Wednesday 18th December 2024, 7.15pm, The Pavilion

193. To note the Environment Coordinator's Update (verbal)

The Environment Coordinator updated the Council on CHEC volunteer group activities (Energy, Food and Growing, Transport, Waste Not Want Not and Wildlife).
Events such as the Swap Shop and community litter picking are well organised and attended. The Wildlife Group continues to be very active; an article written by a local ecologist will appear in the next issue of The Forty with news on the Forty wildflower meadow project. Trees have been planted on the Recreation Ground in collaboration with the Treehouse School and the Green Gym as part of a Trees not Tees initiative. A project proposal for funding under the 'Mend the Gap' initiative is underway and will come to Council for approval when ready. The Transport CHEC group is now a Working Group of the Council helping to deliver transport plan objectives. A first meeting of a Growing Better Together initiative recently took place, bringing interested people together in Cholsey to begin sharing ideas/support. The Energy group needs more volunteers and ideally another Councillor involved to help identify aims and take projects such as Draughtbusters forward.

The Council expressed interest in visits suggested by the Environment Coordinator from a Community Speedwatch officer and the Oxfordshire County Council EV Charging project manager.

A bicycle-powered smoothie maker for use at e.g. the Green Fair will be purchased (rather than continuing to hire) with support of Cholsey's Tomorrow and some funds from the CHEC budget.

The Council expressed appreciation of the Environment Coordinator's work and noted the importance of the role in furthering the new Strategic Plan.

194. To receive update on developing a Community Emergency Plan (Cllrs Herbert and Smith)

Cllrs Smith and Herbert have begun work on a Community Emergency Plan and hope to have this completed and approved by Council by June.

195. To receive update from the Transport Lead (Cllr Collins), in particular:
Councillor Collins reported that despite continued follow up there is no further progress on the A329 crossing proposal. Problems with the zebra crossing lights on Wallingford Road are being followed up with Bellway Homes by Oxfordshire County Council. The status of unadopted roads queried by Cllr Bamford have been clarified. The Clerk will email Councillors asking for another member to join the Transport Working Group.

a. To agree the formation of a Cholsey Station Working Group
It was resolved to form a Cholsey Station Working Group, coordinated by Cllr Collins, to include nominated Council members and other interested Cholsey residents. Cllr Nixon will write to Wallingford Town Council and Benson and Moulsford Parish Councils about the initiative. Cllr Collins has written to David Johnston MP.

196. To receive update from the Staffing Committee (Cllr Finch)
Cllr Finch updated Council following the 28th February Staffing Committee. Draft Minutes of the meeting are available on the Council website.

197. Finance

a. To discuss and agree upon S137 grant request for Cholsey Village CIC (contribution to employment of Children's Centre staff and Mental Health Support Worker)
It was unanimously **resolved** to approve the S137 grant request to Cholsey Village CIC, of £20,000 for 2024/2025, to support the continued operation of the Happy Hub and Mental Health Support drop-in, which are no longer services of the Parish Council.

b. To approve payments made and note payments received
The payments were approved and signed by Cllr Finch and Cllr Herbert.

198. To agree responses to planning applications as at 6th March 2024

P24/S0610/HH	Two storey side extension and single storey rear extension 5 Cross Road It was **resolved** to comment that in line with CNP H7, confirmation is required that sufficient parking will be available with an increase in number of bedrooms.

199. To note planning decisions as at 6th March 2024

P24/S0148/HH	Side extension and porch Meadow Farm, Reading Road **Granted by SODC**
P23/S2272/HH	Dropped kerb access to property 25 Crescent Way **Granted by SODC**

200. Items for information or inclusion on future agenda
Concerns re. bollards, tree planting, and landscaping on Bellway Homes East End estate: Cllr Smith is in touch with the Construction Manager and landowners to resolve these issues.
Emergency Plan
Office revamp
Health and Safety policy
Annual Community meeting
Station Working Group
Estate Manager's update
Councillor co-option

HEALTH AND SAFETY POLICY

1. Introduction

This policy sets out the general principles and approach that the Parish Council will follow in respect of Health and Safety legislation for premises and activities for which the Council is responsible. It is the responsibility of all Councillors and employees of the Council to be aware of the following policy statements on Health and Safety and of the organisational arrangements made to implement these policies.

2. The Parish Council's Health and Safety Policy Statement

2.1. Cholsey Parish Council, in accordance with the requirements of The Health and Safety at Work Act (1974), and The Management of Health and Safety at Work Regulations(1999), accepts its duty to provide and maintain both physically and mentally, safe and healthy working conditions for all its employees. It also accepts its duty of care to other persons such as volunteers and contractors who work on behalf of the Council.

2.2. The Parish Council will take all reasonable steps to ensure that it complies with the law on Health, Safety and Welfare and any relevant Regulations, Approved Codes of Practice and Guidance. It will provide the resources to ensure the safety of its employees and others affected by its work.

2.3. The Parish Council will take all reasonable steps to ensure that:

2.3.1. The information, instruction, training, supervision, equipment and facilities necessary to achieve a safe working environment for employees, members of the public, contractors and volunteers are provided.

2.3.2. Its work, in all its forms, is carried out in ways so that members of the public are not put at risk. Where necessary the Council will obtain specialist technical and Health and Safety advice for any projects or pieces of work that could affect the general public.

2.3.3. Arrangements are in place for the safe use, handling, storage and disposal of all substances and equipment that may endanger health or welfare.

2.3.4. This policy is brought to the attention of employees, members of the public, contractors, volunteers and Councillors and is reviewed periodically.

2.3.5. The Council will actively involve employees in completion of risk assessments connected to their respective roles and encourage employees to raise any health and safety concerns they have with their line manager.

2.3.6. When necessary, there is consultation and negotiation with employees on health,safety and welfare at work to ensure continuing improvement.

2.4. The Parish Council is responsible for managing health and safety, based on the Council's Health and Safety policy.

2.5. The Clerk is responsible for monitoring and reporting to the Council any Health and Safety issues. Day-to-day matters of Health and Safety are dealt with by the Clerk acting on behalf of the Council. The Clerk shall keep copies of all risk assessments, method statements and Health and Safety documents.

2.6. All Councillors, employees/contractors and volunteers have a duty to take reasonable care of their own health and safety and that of any persons who may be affected by their acts or omissions.

3. Risk Assessments

3.1. The Parish Council will carry out risk assessments of its activities as and when necessary and review these annually.

3.2. The Parish Council will set up and monitor policies and procedures to reduce any risks that are identified.

3.3. The Parish Council requires contractors (and venue hirers, where applicable) to supply Risk Assessments, written Method Statements and Safe Systems of Work as appropriate, prior to starting any major works on behalf of the Council.

4. Reporting Accidents

All accidents, no matter how small, involving Employees, Councillors, contractors and volunteers undertaking Council business, and members of the public using Council facilities, must be reported in the first instance to the Clerk and details entered in the Accident Book. Thereafter, all such accidents will be brought to the attention of the Council. In the event of a serious injury or dangerous occurrence, the Chair, or in their absence the Vice Chair will be informed immediately.

5. Review

This document was approved for use at the meeting of the Parish Council on ***xx*** (Minute reference ***yy***), and shall be reviewed at regular intervals and at least annually.

CHOLSEY PARISH COUNCIL

GDPR DATA PROTECTION POLICY

Definitions

In this policy, the following words and phrases have the following meanings:

"Consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

"Criminal records personal data" means personal data relating to criminal convictions and offences and personal data relating to criminal allegations and proceedings.

"Data protection legislation" means the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 and any other applicable primary or secondary legislation as may be in force in the UK from time to time.

"Data subject" means a living identified or identifiable individual about whom the Council holds personal data.

"Member of staff" is any director, employee, worker, agency worker, apprentice, intern, volunteer, contractor and consultant employed or engaged by the Council.

"Personal data" is any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject. It excludes anonymised data, i.e. where all identifying particulars have been removed.

"Processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing or destroying. It also includes transmitting or transferring personal data to third parties.

"Special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning the physical or mental health of a data subject or data concerning a data subject's sex life or sexual orientation.

"Data compliance manager" The Council's data compliance manager has responsibility for data protection compliance within the organisation. The Council's data compliance manager is: The Clerk, Cholsey Parish Council, The Pavilion, Station Road, Cholsey, OX10 9PT; 01491 652255; clerk@cholseyparishcouncil.gov.uk

Introduction

This policy sets out how the Council processes the personal data of data subjects, including the

personal data of job applicants and the personal data of our current and former Councillors, employees, workers, agency workers, apprentices, interns, volunteers, contractors, consultants, clients, suppliers and other third parties.

It applies to all personal data that we process, regardless of the media on which those personal data are stored, e.g. electronically, on paper or on other materials. The Council is committed to being clear and transparent about how we collect and use personal data and to complying with our data protection obligations. Protecting the confidentiality, security and integrity of the personal data that we process is also of paramount importance to our organisation's operations. The Council will process personal data relating to you in accordance with this policy, the data protection legislation and the latest privacy notice which has been issued to you.

This policy applies to all members of staff. It is non-contractual and does not form part of any employment contract, casual worker agreement, consultancy agreement or any other contract for services.

As a member of staff, you are yourself a data subject and you may also process personal data on the Council's behalf about other data subjects. This policy should therefore be read and interpreted accordingly. You must always comply with it when processing personal data on the Council's behalf in the proper performance of your job duties and responsibilities. The data protection legislation contains important principles affecting personal data relating to data subjects. The purpose of this policy is to set out what we expect from you and to ensure that you understand and comply with the rules governing the processing of personal data to which you may have access in the course of your work, so as to ensure that neither the Council nor you breach the data protection legislation.

The Council takes compliance with this policy very seriously. Any breach of this policy or any breach of the data protection legislation will be regarded as misconduct and will be dealt with under the Council's disciplinary procedure. A significant or deliberate breach of this policy, such as accessing a data subject's personal data without authority or unlawfully obtaining or disclosing a data subject's personal data (or procuring their disclosure to a third party) without the Council's consent, constitutes a gross misconduct offence and could lead to your summary dismissal. If you are not an employee, you may have your contract with the Council terminated with immediate effect.

The Council's data compliance manager has responsibility for data protection compliance within the business. You should contact them if you have any questions about the operation of this policy or you need further information about the data protection legislation, or if you have any concerns that this policy is not being or has not been followed.

You must also contact them to seek further advice in the following circumstances:

- if you are in any doubt about what you can or cannot disclose and to whom
- if you are unsure about the lawful basis you are relying on to process personal data
- if you need to rely on consent to process personal data
- if you need to obtain or issue privacy notice
- if you are not clear about the retention period for the personal data being processed
- if you are unsure about what appropriate security measures you need to implement to protect personal data
- if you need assistance in dealing with any rights invoked by a data subject
- if you suspect there has been a personal data breach
- where you propose to use personal data for purposes other than that for which they were

collected
- if you need assistance with, or approval of, contracts in relation to sharing personal data with third-party service providers
- if you believe personal data are not being kept or deleted securely or are being accessed without the proper authorisation
- if you suspect there has been any other breach of this policy or any breach of the data protection principles

If you wish to make an internal complaint that this policy is not being or has not been followed, you can also raise this as a formal grievance under the Council's grievance procedure.

The data protection principles

Under the data protection legislation, there are six data protection principles that the Council and all members of staff must comply with at all times in their personal data processing activities. In brief, the principles say that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

2. Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

4. Accurate and, where necessary, kept up to date; every reasonable step must also be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (storage limitation).

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

The Council is responsible for, and must be able to demonstrate compliance with, these data protection principles. This is called the principle of accountability.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

This principle means that both the Council and members of staff may only collect, process and share personal data lawfully and fairly and for specific purposes.

Lawfulness and fairness

The data protection legislation provides that processing is only lawful in certain circumstances. These include where:

- the data subject has given consent to the processing of their personal data for one or more specific purposes
- the processing is necessary for the performance of a contract with the data subject, e.g. an employment contract, or in order to take steps at the request of the data subject prior to entering into a contract
- the processing is necessary for compliance with our legal obligations
- the processing is necessary to protect the data subject's vital interests (or someone else's vital interests)
- the processing is necessary to pursue our legitimate interests (or those of a third party), where the data subject's interests or fundamental rights and freedoms do not override our interests; the purposes for which we process personal data for legitimate interests must also be set out in an appropriate privacy notice

The Council and members of staff must only process personal data on the basis of one or more of these lawful bases for processing. Before a processing activity starts for the first time, and then regularly while it continues, we will review the purpose of the processing activity, select the most appropriate lawful basis (or bases) for that processing and satisfy ourselves that the processing is necessary for the purpose of that lawful basis (or bases). When determining whether the Council's legitimate interests are the most appropriate basis for lawful processing, we will conduct a legitimate interests assessment, keep a record of it and keep it under review.

Where the Council relies on consent as the lawful basis for processing, this requires the data subject to have given a positive statement, active opt-in or clear affirmative action; pre-ticked boxes, inactivity or silence do not constitute consent. If consent is given in a document that also deals with other matters, the request for consent must be clearly distinguishable and kept separate from those other matters. In addition, consent must specifically cover the purposes of the processing and the types of processing activity, so you must ensure that you obtain separate consents for different types of processing, where appropriate. Data subjects also have the right to withdraw their consent to processing at any time, they must be advised of this right and it must be as easy for them to withdraw their consent as it was to give it.

The data protection legislation also provides that the processing of special categories of personal data and criminal records personal data is only lawful in more limited circumstances where a special condition for processing also applies (this is an additional requirement; the processing must still meet one or more of the conditions for processing set out above). These include where:

- the data subject has given their explicit consent to the processing of their personal data for one or more specified purposes; explicit consent requires a very clear and positive statement and it cannot be implied from the data subject's actions
- the processing is necessary for the purposes of carrying out obligations or exercising specific rights of either the Council or the data subject under employment law or social security law
- in the case of special categories of personal data, the processing relates to personal data which are manifestly made public by the data subject
- the processing is necessary for the establishment, exercise or defence of legal claims

The Council may from time to time need to process special categories of personal data and criminal records personal data. The Council and members of staff must only process special categories of personal data and criminal records personal data where there is also one or more of these special lawful bases for processing. Before processing any special categories of personal data and criminal records personal data, you must notify our data compliance manager so that they may assess whether the processing complies with one or more of these special conditions.

A clear record must be kept of all consents, including explicit consents, which covers what the data subject has consented to, what they were told at the time and how and when consent was given. This enables the Council to demonstrate compliance with the data protection requirements for consent.

Transparency

Under the data protection legislation, the transparency principle requires the Council to provide specific information to data subjects through appropriate privacy notices. These must be concise, transparent, intelligible, easily accessible and use clear and plain language. Privacy notices may comprise general privacy statements applicable to a specific group of data subjects, e.g. employees, or they may be stand-alone privacy statements covering processing related to a specific purpose. Whenever we collect personal data directly from data subjects, including for employment purposes, we must provide the data subject with all the information required to be included in a privacy notice. This includes:

- the identity and contact details of the Council (as data controller) and any representative
- the purposes for which the personal data will be processed
- the lawful basis or bases for processing
- where we are relying on our legitimate interests (or those of a third party) as the lawful basis for processing, what those legitimate interests are
- the categories of personal data, unless they were obtained directly from the data subject
- the third-party sources that the personal data originate from, unless they were obtained directly from the data subject
- the recipients, or categories of recipients, with whom the personal data may be shared
- details of transfers to non-EEA countries and the suitable safeguards applied
- the retention period for the personal data or, if that is not possible, the criteria to be used to determine the retention period
- the existence of the data subject's rights, i.e. subject access, rectification, erasure, restriction of processing, objection and data portability
- the right to withdraw consent to processing at any time, where consent is being relied on as the lawful basis for processing
- the right to lodge a complaint with the Information Commissioner's Office
- whether the provision of personal data is part of a statutory or contractual requirement or obligation, or a requirement necessary to enter into a contract, and the possible consequences of failing to provide the personal data
- the existence of any automated decision-making, including profiling, and meaningful information about how decisions are made, the significance and consequences.

We must issue a privacy notice, which can be by electronic means, when we first collect a data subject's personal data from them. If the personal data have been obtained from third parties, we must provide the privacy notice information within a reasonable period of having obtained the personal data, but at the latest within one month. However, if the personal data are to be used to communicate with the data subject, the privacy notice information is to be provided, at the latest, when the first communication takes place, or if disclosure of the personal data to another recipient is envisaged, it is to be provided, at the latest, when the data are first disclosed. You must comply with these rules on privacy notices when processing personal data on the Council's behalf in the proper performance of your job duties and responsibilities.

The Council will issue privacy notices to you from time to time.

Privacy notices can also be obtained from the Council's data compliance manager.

Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes and they must not be further processed in any manner that is incompatible with those purposes.

Personal data cannot be used for new, different or incompatible purposes from those disclosed to the data subject when they were first obtained, for example in an appropriate privacy notice, unless the data subject has been informed of the new purposes and the terms of this policy are otherwise complied with, e.g. there is a lawful basis for processing. This also includes special categories of personal data and criminal records personal data.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

We will only collect personal data to the extent that they are required for the specific purposes notified to the data subject. You must only process personal data where your job duties and responsibilities require it and you must not process personal data for any reason which is unrelated to your job duties and responsibilities. In addition, you must ensure that any personal data you collect are adequate and relevant for the intended purposes and are not excessive. This includes special categories of personal data and criminal records personal data.

When personal data are no longer needed for specified purposes, you must ensure that they are destroyed, erased or anonymised in accordance with the Council's rules on data retention and destruction set out below.

Accuracy

Personal date must be accurate and, where necessary, kept up to date. In addition, every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

It is important that the personal data we hold about you as a data subject is accurate and up to date. Please keep us informed if your personal data changes, e.g. you change your home address, so that our records can be updated. The Council cannot be held responsible for any errors in your personal data in this regard unless you have notified the Council of the relevant change. We will promptly update your personal data if you advise us that they have changed or are inaccurate.

You must also ensure that the personal data we hold about other data subjects is accurate and up to date where this is part of your job duties or responsibilities. This includes special categories of personal data and criminal records personal data. You must check the accuracy of any personal data at the point of their collection and at regular intervals thereafter. You must take all reasonable steps to destroy, erase or update outdated personal data and to correct inaccurate personal data.

Storage limitation

Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.

The Council will only retain personal data for as long as is necessary to fulfil the legitimate business purposes for which they were originally collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements. This includes

special categories of personal data and criminal records personal data. You must comply with the Council's rules on data retention and destruction set out below.

Retention: job applicants

If a job applicant's application for employment or engagement is unsuccessful, the Council will generally hold their personal data, including special categories of personal data and criminal records personal data, for six months after the end of the relevant recruitment exercise but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal data for up to six years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court.

If the job applicant has consented to the Council keeping their personal data on file for in case there are future suitable employment opportunities with us, we will hold their personal data for a further six months after the end of the relevant recruitment exercise, or until they withdraw their consent if earlier.

Retention: members of staff

The Council will generally hold personal data, including special categories of personal data and criminal records personal data, for the duration of a member of staff's employment or engagement. The exceptions are:

- any personal data supplied as part of the recruitment process will not be retained if they have no bearing on the ongoing working relationship
- criminal records personal data collected in the course of the recruitment process will be deleted once they have been verified through a DBS criminal record check, unless, in exceptional circumstances, the information has been assessed by the Council as relevant to the ongoing working relationship
- it will only be recorded whether a DBS criminal record check has yielded a satisfactory or unsatisfactory result, unless, in exceptional circumstances, the information in the criminal record check has been assessed by the Council as relevant to the ongoing working relationship
- if it has been assessed as relevant to the ongoing working relationship, a DBS criminal record check will nevertheless be deleted after once the conviction is "spent" (unless information about spent convictions may be retained because the role is an excluded occupation or profession)
- disciplinary, grievance and capability records will only be retained until the expiry of any warning given (but a summary disciplinary, grievance or performance management record will still be maintained for the duration of employment).

Once a member of staff has left employment or their engagement has been terminated, we will generally hold their personal data, including special categories of personal data and criminal records personal data, for one year after the termination of their employment or engagement, but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal data for up to six years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court. We will hold payroll, wage and tax records (including salary, bonuses, overtime, expenses, benefits and pension information, National Insurance number, PAYE records, tax code and tax status information) for up to six years after the termination of their employment or engagement.

Overall, this means that we will "thin" the file of personal data that we hold on members of staff

one year after the termination of their employment or engagement, so that we only continue to retain for a longer period what is strictly necessary.

Retention: other third parties, including clients, customers and suppliers

The Council will generally hold personal data, including special categories of personal data and criminal records personal data, belonging to clients, customers and suppliers for the duration of our business relationship with them.

Once our organisation's relationship with a client or supplier has been terminated, we will generally hold their personal data, including special categories of personal data and criminal records personal data, for one year after the termination of the business relationship, but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal data for up to six years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a County Court or High Court.

Overall, this means that we will "thin" the file of personal data that we hold on clients and suppliers one year after the termination of the relationship, so that we only continue to retain for a longer period what is strictly necessary.

Destruction and erasure

All personal data, including special categories of personal data and criminal records personal data, must be reviewed before destruction or erasure to determine whether there are special factors that mean destruction or erasure should be delayed. Otherwise, they must be destroyed or erased at the end of the retention periods outlined above. If you are responsible for maintaining personal data and are not clear what retention period should apply to a particular record, please contact our data compliance manager for guidance.

Personal data which are no longer to be retained will be permanently erased from our IT systems or securely and effectively destroyed, e.g. by cross-shredding of hard copy documents, burning them or placing them in confidential waste bins or by physical destruction of storage media, and we will also require third parties to destroy or erase such personal data where applicable. You must take all reasonable steps to destroy or erase personal data that we no longer require.

In some circumstances we may anonymise personal data so that they no longer permit a data subject's identification. In this case, we may retain such personal data for a longer period.

Integrity and confidentiality

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

The Council takes the security of personal data seriously and we have implemented and maintain safeguards which are appropriate to the size and scope of our business, the amount of personal data that we hold and any identified risks. This includes encryption and pseudonymisation of personal data where appropriate. We have also taken steps to ensure the ongoing confidentiality, integrity, availability and resilience of our processing systems and services and to ensure that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner. We regularly test and evaluate the effectiveness of our technical and organisational safeguards to ensure the security of our processing activities.

In turn, you are responsible for protecting the personal data that we hold, and you must implement reasonable and appropriate security measures against unauthorised or unlawful processing of personal data and against their accidental loss, destruction or damage. You must be particularly careful in protecting special categories of personal data and criminal records personal data. You must follow all procedures, and comply with all technologies and safeguards, that we put in place to maintain the security of personal data from the point of collection to the point of destruction.

Where the Council uses third-party service providers to process personal data on our behalf, additional security arrangements need to be implemented in contracts with those third parties to safeguard the security of personal data. You can only share personal data with third-party service providers if you have been authorised to do so and provided that certain safeguards and contractual arrangements have been put in place, including that:

- the third party has a business need to know the personal data for the purposes of providing the contracted services
- sharing the personal data complies with the privacy notice that has been provided to the data subject (and, if required, the data subject's consent has been obtained)
- the third party has agreed to comply with our data security procedures and has put adequate measures in place in ensure the security of processing
- the third party only acts on our documented written instructions
- a written contract is in place between the Council and the third party that contains specific approved terms
- the third party will assist the Council in allowing data subjects to exercise their rights in relation to data protection and in meeting our obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments
- the third party will delete or return all personal data to the Council at the end of the contract
- the third party will submit to audits.

Before any new agreement involving the processing of personal data by a third-party service provider is entered into, or an existing contract is amended, you must seek the approval of its terms from our data compliance manager.

You may only share personal data with other members of staff if they have a business need to know in order to properly perform their job duties and responsibilities.

Hard copy personnel files, which hold personal data gathered during the working relationship, are confidential and must be stored in locked filing cabinets. Only authorised members of staff, who have a business need to know in order to properly perform their job duties and responsibilities, have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on removable storage media must be kept in locked filing cabinets or locked drawers and cupboards when not in use by authorised members of staff. Personal data held in electronic format will be stored confidentially by means of password protection, encryption or pseudonymisation, and again only authorised members of staff have access to those data.

The Council has network backup procedures in place to ensure that personal data held in electronic format cannot be accidentally lost, destroyed or damaged. Personal data must not be stored on local computer drives or on personal devices.

The data protection legislation requires the Council to notify any personal data breach to the Information Commissioner's Office within 72 hours after becoming aware of the breach and, where there is a high risk to the rights and freedoms of data subjects, to the data subject themselves. A

personal data breach is any breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and includes any act or omission that compromises the confidentiality, integrity or availability of personal data or the safeguards that we, or our third-party service providers, have put in place to protect them. The Council has procedures in place to deal with any suspected personal data breach and you are required to comply with these. If you know or suspect that a personal data breach has occurred, you must immediately contact our data compliance manager, retain any evidence you have in relation to the breach and follow the Council's data breach policy and response plan.

Accountability

The Council is responsible for, and must be able to demonstrate compliance with, the data protection principles. This means that we must implement appropriate and effective technical and organisational measures to ensure compliance and we also require you to fully assist and co-operate with us in this regard. In particular, we have:

- appointed a data compliance manager to be responsible for data protection compliance and privacy matters within the business
- kept written records of personal data processing activities
- implemented a privacy by design approach when processing personal data and we will conduct and complete data protection impact assessments (DPIAs) where a type of data processing, e.g. the launch of a new product or the adoption of a new program, process or IT system, in particular using a new technology, is likely to result in a high risk to the rights and freedoms of data subjects
- integrated data protection requirements into our internal documents, including this data protection policy, other related policies and privacy notices
- introduced a regular training programme for all members of staff on the data protection legislation and on their data protection duties and responsibilities and we also maintain a training record to monitor its delivery and completion – you must undergo all mandatory data protection training
- introduced regular reviews of our privacy measures and our policies, procedures and contracts and regular testing of our systems and processes to monitor and assess our ongoing compliance with the data protection legislation and the terms of this policy in areas such as security, retention and data sharing.

We also keep records of our personal data processing activities and you are required to assist us in ensuring these records are full, accurate and kept up to date.

Privacy by design and data protection impact assessments

We are required to implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the data protection legislation. You must assess what privacy by design measures can be implemented on all processes or systems that process personal data where this is part of your job duties or responsibilities because those processes or systems are under your control.

Where a type of data processing, e.g. the launch of a new product or the adoption of a new program, process or IT system which is under your control, is likely to result in a high risk to the rights and freedoms of data subjects, you must assist us in conducting and completing a DPIA. This includes (but is not limited to):

- systematic and extensive automated processing and automated decision-making activities, including profiling, and on which decisions are based that have legal effects, or similar significant effects, on data subjects
- large-scale processing of special categories of personal data or criminal records personal data
- large-scale systematic monitoring of publicly accessible areas, e.g. using CCTV.

Before any form of new technology, program, process or system is introduced, you must contact our data compliance manager in order that a DPIA can be carried out.

A DPIA will comprise a review of the new technology, program, process or system and it must contain a description of the processing operations and the purposes, an assessment of the necessity and proportionality of the processing in relation to those purposes, an assessment of the risks to individuals and the measures in place to address or mitigate those risks and demonstrate compliance.

Automated processing and automated decision-making

Automated processing is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, and automated decision-making occurs when an electronic system uses an individual's personal data to make a decision without human intervention.

The Council does not carry out any automated processing and does not take any decisions based solely on automated decision-making, including profiling.

Direct marketing

The Council is subject to certain rules if marketing to clients. If you are involved in direct marketing to clients, you must comply with the Council's guidelines on this. In particular, a data subject's prior consent is required for electronic direct marketing. There is a limited exception for existing clients which allows us to send marketing texts and e-mails if we have obtained their contact details in the course of a sale to that person, we are marketing similar services to them and we gave that person an opportunity to opt out of marketing when first collecting their details and in every subsequent message.

If a data subject objects to direct marketing, it is essential that this is actioned in a timely manner and their details should be suppressed as soon as possible. You can retain just enough information to ensure that marketing preferences are respected in the future.

Transferring personal data outside the European Economic Area

The data protection legislation restricts transfers of personal data to countries outside the European Economic Area (EEA) in order to ensure that the level of data protection afforded to data subjects is maintained.

The Council does not transfer personal data to countries outside the EEA and you must ensure that you comply with this rule.

Data subject rights to access personal data

Under the data protection legislation, data subjects have the right, on request, to obtain a copy of the personal data that the Council holds about them by making a written data subject access request (DSAR). This allows the data subject to check that we are lawfully processing their personal data.

The data subject has the right to obtain:

- confirmation as to whether or not their personal data are being processed
- access to copies of their specified personal data
- other additional information.

The other additional information (which should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language) comprises:

- the purposes of the processing and the categories of personal data concerned
- the recipients, or categories of recipients, to whom the personal data have been or will be disclosed, in particular recipients in non-EEA countries
- where the personal data are transferred to a non-EEA country, what appropriate safeguards are in place relating to the transfer
- the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- the existence of the data subject's rights to request rectification or erasure of their personal data or restriction of processing of their personal data or to object to such processing
- their right to lodge a complaint with the Information Commissioner's Office if they think the Council has failed to comply with their data protection rights
- where the personal data are not collected from them, any available information as to their source
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the envisaged consequences of such processing for them.

When a data subject makes a DSAR, we will log the date on which the request was received and confirm their identity. Where we have reasonable doubts concerning the data subject's identity, we will request them to provide such additional information necessary to confirm their identity before complying with their DSAR. We will then search databases, systems and other places where the personal data which are the subject of the DSAR may be held. Where we process a large quantity of personal data about a data subject, we may ask them to first specify the information that their DSAR relates to.

If the data subject makes their DSAR electronically, the Council must provide a copy of the personal data in a commonly used electronic format, unless they specifically request otherwise. If the data subject wants additional copies of the personal data, the Council will charge a reasonable fee, which is based on our administrative costs of providing the additional copies.

The Council will normally respond to a DSAR and provide copies of the personal data within one month of the date of receipt of the request. However, we may extend this time limit for responding by a further two months if the request is complex or there are a number of requests made by the data subject. If we intend to extend the time limit, we will contact the data subject within one month of the DSAR's receipt to inform them of the extension and to explain why it is necessary.

Before providing the personal data to the data subject making the DSAR, we will review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data. We will also check whether there are any statutory exemptions from disclosure that apply to the personal data that are the subject of the DSAR. If a statutory exemption applies to any of the personal data, those personal data may not be disclosed.

Whilst we will normally provide a copy of the personal data in response to a DSAR free of charge,

we reserve the right to charge a reasonable fee, based on our administrative costs of providing the personal data, when a DSAR is manifestly unfounded or excessive, particularly if it repeats a DSAR to which we have already responded. Alternatively, where a DSAR is manifestly unfounded or excessive, we reserve the right to refuse to respond altogether. Where we refuse to act on a request in this way, we will set out our written reasons why to the data subject within one month of receipt of their DSAR. We will also inform them of their right to complain to the Information Commissioner's Office or to seek a judicial remedy in the courts.

If you wish to exercise your data subject access rights, please complete our data subject access request form, or put the request in an e-mail, and send it to our data compliance manager. We will inform you if we need to further verify your identity.

If you receive a DSAR from another data subject, you must immediately forward it to our data compliance manager and they will deal with responding to it.

Other data subject rights in relation to their personal data

Data subjects have a number of other rights in relation to their personal data. When we process data subjects' personal data, we will respect those rights. It is the Council's policy to ensure that requests by data subjects to exercise their rights in respect of their personal data are handled in accordance with the data protection legislation.

Subject to certain conditions, and in certain circumstances, data subjects have the right to:

- be informed – this is normally satisfied by issuing them with an appropriate privacy notice
- request rectification of their personal data - this enables them to have any inaccurate or incomplete personal data we hold about them corrected or completed, including by their providing a supplementary statement
- request the erasure of their personal data - this enables them to ask us to delete or remove their personal data where there's no compelling reason for their continued processing, e.g. it's no longer necessary in relation to the purpose for which they were originally collected or if there are no overriding legitimate grounds for the processing
- restrict the processing of their personal data - this enables them to ask us to suspend the processing of their personal data, e.g. if they contest the accuracy and so want us to verify the accuracy or the processing is unlawful but they don't want the personal data to be erased
- object to the processing of their personal data - this enables them to ask us to stop processing their personal data where we are relying on the legitimate interests of the business as our lawful basis for processing and there is something relating to their particular situation which makes them decide to object to processing on this ground
- data portability - this gives them the right to request the transfer of their personal data to another party so that they can reuse them across different services for their own purposes
- not be subject to automated decision-making, including profiling - this gives them the right not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them
- prevent direct marketing - this enables them to prevent our use of their personal data for direct marketing purposes
- be notified of a data breach which is likely to result in a high risk to their rights and freedoms.

If, as a data subject, you wish to exercise any of these rights, please contact data compliance manager.

If a data subject invokes any of these rights, you must take steps to verify their identity, log the

date on which the request was received and seek advice from our data compliance manager if you need assistance in dealing with the matter. The following response procedures apply as applicable:

- response to requests to rectify personal data - unless there is an applicable exemption, we will rectify the personal data without undue delay and we will also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed, e.g. our third-party service providers, unless this is impossible or involves disproportionate effort
- response to requests for the erasure of personal data - we will erase the personal data without undue delay provided one of the grounds set out in the data protection legislation applies and there is no applicable exemption (and, where the personal data are to be erased, a similar timetable and procedure to that applying to responding to DSARs will be followed). We will also communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. Where we have made the personal data public, we will take reasonable steps to inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data
- response to requests to restrict the processing of personal data - where processing has been restricted in accordance with the grounds set out in the data protection legislation, we will only process the personal data (excluding storing them) with the data subject's consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another person, or for reasons of important public interest. Prior to lifting the restriction, we will inform the data subject that it is to be lifted. We will also communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort
- response to objections to the processing of personal data - where such an objection is made in accordance with the data protection legislation and there is no applicable exemption, we will no longer process the data subject's personal data unless we can show compelling legitimate grounds for the processing which overrides the data subject's interests, rights and freedoms or we are processing the personal data for the establishment, exercise or defence of legal claims. If a data subject objects to the processing of their personal data for direct marketing purposes, we will stop processing the personal data for such purposes
- response to requests for data portability - unless there is an applicable exemption, we will provide the personal data without undue delay if the lawful basis for the processing of the personal data is consent or pursuant to a contract and our processing of those data is carried out by automated means (and a similar timetable and procedure to that applying to responding to DSARs will be followed)

In the limited circumstances where the data subject has provided their consent to the processing of their personal data for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. This will not, however, affect the lawfulness of processing based on consent before its withdrawal.

If, as a data subject, you wish to withdraw your consent to the processing of your personal data for a specific purpose, please contact our data compliance manager. Once we have received notification that you have withdrawn your consent, we will no longer process your personal data for the purpose you originally agreed to, unless we have another lawful basis for processing.

If a data subject invokes their right to withdraw their consent, seek advice from our data compliance manager if you need assistance in dealing with the matter.

Data subjects also have the right to make a complaint to the Information Commissioner's Office at any time.

Your obligations in relation to personal data

You must comply with this policy and the data protection principles at all times in your personal data processing activities where you are acting on behalf of the Council in the proper performance of your job duties and responsibilities. We rely on you to help us meet our data protection obligations to data subjects.

Under the data protection legislation, you should also be aware that you are personally accountable for your actions and you can be held criminally liable. It is a criminal offence for you knowingly or recklessly to obtain or disclose personal data (or to procure their disclosure to a third party) without the consent of the Council. This would include, for example, taking clients' contact details or other personal data without the Council's consent on the termination of your employment, accessing another employee's personal data without authority or otherwise misusing or stealing personal data held by the Council. It is also a criminal offence to knowingly or recklessly re-identify personal data that has been anonymised without the consent of the Council, where we de-identified the personal data, and it is a criminal offence to alter, block, erase, destroy or conceal personal data with the intention of preventing their disclosure to a data subject following a data subject access request. Where unlawful activity is suspected, the Council will report the matter to the Information Commissioner's Office for investigation into the alleged breach of the data protection legislation and this may result in criminal proceedings being instigated against you. The Council may also need to report the alleged breach to a regulatory body. This conduct would also amount to a gross misconduct offence under the Council's disciplinary procedure and could lead to your summary dismissal.

You must also comply with the following guidelines at all times:

- only access personal data that you have authority to access and only for authorised purposes, e.g. if you need them for the work you do for the Council, and then only use the data for the specified lawful purpose for which they were obtained
- only allow other members of staff to access personal data if they have the appropriate authorisation and never share personal data informally
- do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Council's website or posted on the Internet in any form, unless the data subject has given their explicit consent to this
- be aware that those seeking personal data sometimes use deception to gain access to them, so always verify the identity of the data subject and the legitimacy of the request
- where the Council provides you with code words or passwords to be used before releasing personal data, you must strictly follow the Council's requirements in this regard
- only transmit personal data between locations by e-mail if a secure network is in place, e.g. encryption is used for e-mail
- if you receive a request for personal data about another member of staff or data subject, you should forward this to the Council's data compliance manager
- ensure any personal data you hold are kept securely, either in a locked non-portable filing cabinet or drawer if in hard copy, or password protected or encrypted if in electronic format, and comply with Council rules on computer access and secure file storage
- do not access another member of staff's personal data, e.g. their personnel records, without authority as this will be treated as gross misconduct and it is a criminal offence
- do not obtain or disclose personal data (or procure their disclosure to a third party) without authority or without the Council's consent as this will be treated as gross misconduct and it is a criminal offence
- do not write down (in electronic or hard copy form) opinions or facts concerning a data subject

which it would be inappropriate to share with that data subject

- do not remove personal data, or devices containing personal data, from the workplace with the intention of processing them elsewhere unless this is necessary to enable you to properly carry out your job duties and responsibilities, you have adopted appropriate security measures (such as password protection, encryption or pseudonymisation) to secure the data and the device and it has been authorised by your line manager
- ensure that, when working on personal data as part of your job duties and responsibilities when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security
- do not store personal data on local computer drives, your own personal computer or on other personal devices
- do not make unnecessary copies of personal data and keep and dispose of any copies securely, e.g. by cross-shredding hard copies
- ensure that you attend all mandatory data protection training
- refer any questions that you may have about the data protection legislation or compliance with this policy to our data compliance manager
- remember that compliance with the data protection legislation and the terms of this policy is your personal responsibility.

Changes to this policy

The Council will review this policy at regular intervals and we reserve the right to update or amend it at any time and from time to time. We will circulate any modified policy to members of staff and, where appropriate, we may notify you of changes by e-mail.

It is intended that this policy is fully compliant with the data protection legislation. However, if any conflict arises between the data protection legislation and this policy, the Council will comply with the data protection legislation.

This policy may also be made available to the Information Commissioner's Office on request.

CHOLSEY PARISH COUNCIL

GDPR DATA BREACH POLICY AND RESPONSE PLAN

Introduction

Under the General Data Protection Regulation (GDPR), certain personal data breaches must be notified to the Information Commissioner's Office (ICO) and sometimes affected data subjects need to be told too.

The purpose of this policy is to outline the Council's internal breach reporting procedure and the Council's internal and external response plan and it should be read in conjunction with the Council's data protection policy.

What constitutes a personal data breach?

A personal data breach is a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*.

A breach is therefore a type of security incident and there are three different types of breaches that may occur:

1. Confidentiality breach - an accidental or unauthorised disclosure of, or access to, personal data.
2. Availability breach - an accidental or unauthorised loss of access to, or destruction of, personal data.
3. Integrity breach - an accidental or unauthorised alteration of personal data.

A breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

A personal data breach would, for example, include:

- loss of personal data, e.g. loss or theft of a Council smartphone or laptop which holds personal data such as a client database, or where the only copy of personal data has been encrypted by ransomware and the data cannot be restored from backup
- personal data being disclosed to an unauthorised person, e.g. an employee's payslip being sent to the wrong person
- an unauthorised person accessing personal data, e.g. an employee's personnel file being inappropriately accessed by another member of staff due to a lack of appropriate internal controls
- a temporary or permanent loss of access to personal data, e.g. where a client's or customer's personal data is unavailable for a certain period of time due to a system shut down, power, hardware or software failure, infection by ransomware or viruses or denial of service attack, where personal data has been deleted either accidentally due to human error or by an unauthorised person or where the decryption key for securely encrypted data has been lost.

This list is not exhaustive.

Notification to the ICO

Not all personal data breaches have to be notified to the ICO. The breach will only need to be notified if it is likely to result in a risk to the rights and freedoms of data subjects, and this needs to be assessed by the Council on a case-by-case basis. A breach is likely to result in a risk to the rights and freedoms of data subjects if, for example, it could result in:

- loss of control over their data
- limitation of their rights
- discrimination
- identity theft
- fraud
- damage to reputation
- financial loss
- unauthorised reversal of pseudonymisation
- loss of confidentiality
- any other significant economic or social disadvantage.

Where a breach is reportable, the Council must notify the ICO without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If the Council's report is submitted late, it must also set out the reasons for the delay. Notification must at least include:

- a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records
- the name and contact details of the Council's data compliance manager
- a description of the likely consequences of the breach
- a description of the measures taken, or to be taken, by the Council to address the breach and mitigate its possible adverse effects.

The Council can provide this information in phases, without undue further delay, if it cannot all be provided at the same time.

Awareness of the breach occurs when the Council has a reasonable degree of certainty that a breach has occurred. In some cases, it will be relatively clear from the outset that there has been a breach.

However, where it is unclear whether or not a breach has occurred, the Council will have a short period of time to carry out an initial investigation after first being informed about a potential breach in order to establish with a reasonable degree of certainty whether or not a breach has in fact occurred.

If, after this short initial investigation, it is established that there is a reasonable degree of likelihood that a breach has occurred, the 72 hours starts to run from the moment of that discovery.

Communication to affected data subjects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Council also needs to communicate the breach to the affected data subjects without undue delay, i.e. as soon as possible. In clear and plain language, the Council must provide them with:

- a description of the nature of the breach

- the name and contact details of the Council's data compliance manager
- a description of the likely consequences of the breach
- a description of the measures taken, or to be taken, by the Council to address the breach and mitigate its possible adverse effects.

The Council will also endeavour to provide data subjects with practical advice on how they can themselves limit the damage, e.g. cancelling their credit cards or resetting their passwords.

The Council will contact data subjects individually, which may be by letter, e-mail or text message, unless that would involve the Council in disproportionate effort, such as where their contact details have been lost as a result of the breach or were not known in the first place, in which case the Council will use a public communication, such as a notification on the Council's website, issuing a public statement or a prominent advertisement in print media.

However, the Council does not need to report the breach to data subjects if:

- the Council has implemented appropriate technical and organisational protection measures, and those measures have been applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as state-of-the-art encryption, or
- the Council has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

Assessing "risk" and "high risk"

In assessing whether a personal data breach results in a risk or high risk to the rights and freedoms of data subjects, the Council will take into account the following criteria:

- the type of breach
- the nature, sensitivity and volume of personal data affected
- ease of identification of data subjects - properly encrypted data is unlikely to result in a risk if the decryption key was not compromised in the breach
- the severity of the consequences for data subjects
- any special characteristics of the data subject
- the number of affected data subjects
- special characteristics of the Council.

Data breach register

The Council will maintain a register of all personal data breaches, regardless of whether or not they are notifiable to the ICO. The register will include a record of:

- the facts relating to the breach, including the cause of the breach, what happened and what personal data were affected
- the effects of the breach
- the remedial action the Council has taken.

Data breach reporting procedure

If you know or suspect that a personal data breach has occurred, you must immediately both advise your line manager and contact the Council's data compliance manager. They can be contacted as follows: The Clerk, Cholsey Parish Council, The Pavilion, Station Road, Cholsey, OX10 9PT;

01491 652255; clerk@cholseyparishcouncil.gov.uk. You must ensure you retain any evidence you have in relation to the breach and you must provide a written statement setting out any relevant information relating to the actual or suspected personal data breach, including:

- your name, department and contact details
- the date of the actual or suspected breach
- the date of your discovery of the actual or suspected breach
- the date of your statement
- a summary of the facts relating to the actual or suspected breach, including the types and amount of personal data involved
- what you believe to be the cause of the actual or suspected breach
- whether the actual or suspected breach is ongoing
- who you believe may be affected by the actual or suspected breach.

You must then follow the further advice of the data compliance manager. You must never attempt to investigate the actual or suspected breach yourself and you must not attempt to notify affected data subjects. The Council will investigate and assess the actual or suspected personal data breach in accordance with the response plan set out below and the data breach team will determine who should be notified and how.

Response plan

The Council's data compliance manager will assemble a team to investigate, manage and respond to the personal data breach. They will lead this team and the other members will consist of nominated Employees and Councillors. The data breach team will then:

1. Make an urgent preliminary assessment of what data has been lost, why and how.
2. Take immediate steps to contain the breach and recover any lost data.
3. Undertake a full and detailed assessment of the breach.
4. Record the breach in the Council's data breach register.
5. Notify the ICO where the breach is likely to result in a risk to the rights and freedoms of data subjects.
6. Notify affected data subjects where the breach is likely to result in a high risk to their rights and freedoms.
7. Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist the data breach team in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of data subjects.

Example	**Notify the ICO?**	**Notify data subjects?**	**Notes**
The Council stored a backup of an archive of personal data encrypted on a CD and the CD is stolen during a burglary	No	No	As long as the personal data are encrypted with a state-of-the-art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required
Personal data are exfiltrated from a secure website managed by the Council during a cyber-attack	Yes, if there are potential consequences to individuals	Yes, depending on the nature of the personal data affected and if the severity of the potential consequences to data subjects is high	If the risk is not high, the Council can still notify data subjects, depending on the circumstances of the case
A brief power outage lasting several minutes means that clients are unable to call the Council and access their records	No	No	This is not a notifiable personal data breach, but it is still a recordable incident
The Council suffers a ransomware attack which results in all personal data being encrypted, no backups are available and the personal data cannot be restored On investigation, it becomes clear that the ransomware's only functionality was to encrypt the personal data, and that there was no other malware present in the	Yes, if there are potential consequences to individuals as this is a loss of availability	Yes, depending on the nature of the personal data affected and the possible effect of the lack of availability of the personal data, as well as other likely consequences	If there was a backup available and personal data could be restored in good time, this would not need to be reported to the ICO or to data subjects as there would have been no permanent loss of availability or confidentiality

system			
An employee reports that they have received a monthly payslip for another employee and a short investigation reveals that it is a systemic flaw and other employees may be affected	Yes	Only if there is high risk	If, after further investigation, it is identified that more employees are affected, an update to the ICO must be made and the Council must take the additional step of notifying those other data subjects if there is high risk to them
The Council's website suffers a cyber-attack and customers' login usernames, passwords and purchase history are published online by the attacker	Yes	Yes, as could lead to high risk	The Council should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk
Clients' personal data are mistakenly sent to the wrong mailing list	Yes	Yes, depending on the scope and type of personal data involved and the severity of possible consequences	
A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the e-mail address of other recipients	Yes, notifying may be obligatory if a large number of individuals are affected, if sensitive personal data are revealed or if other factors present high risks, e.g. the e-mail contains passwords	Yes, depending on the scope and type of personal data involved and the severity of possible consequences	Notification may not be necessary if no sensitive personal data is revealed and if only a minor number of e-mail addresses are revealed

Estate Manager's Report to Parish Council April 2024

Hedges

Work on hedges has now stopped for the nesting season.

We will be monitoring the growth and by autumn will understand if new hedging whips will need to be planted.

Allotments

Invoices for the annual allotment rents were sent out at the beginning of April via email.

The skips were very well received and were unfortunately overloaded, as such the skip company left some waste behind. This proved to be an issue at the Cholsey Meadows site as more rubbish accumulated, some fly tipping, and we had pay for this to be removed by a contractor.

The unused plots have been cleared and we have had a couple of tenancy terminations. I am in the process of offering the plots to people on the waiting lists which is going down very well.

Recreation Grounds and Play Areas.

Cholsey Bluebirds Football

No update as yet.

Recreation Ground

The outdoor table tennis table has been delivered, assembled and installed on 08/04/2024.

Playgrounds

The annual inspection of the play equipment, including the new outdoor gym equipment, took place at the end of February.

Cholsey Meadows Play Area

The wooden picket fence around the play area, including two gates, has now been replaced.

Please note the inspection report regarding the play equipment at Cholsey Meadows, in particular:

P11 – the Fort – Finding 7 and also P30, their recommendations.

P14 – the Ship - Finding 1 and also P42, their recommendations.

I drew attention to these two pieces of equipment previously as the wood was rotten to some depth and recommended they be replaced. There have since been some repairs made by Vistry and Home Front.

Station Road Play Area.

We have eventually been informed by Hags that the parts needed for the repairs to the recreation ground play equipment will take 2 weeks. However, the basketball back board has to be purchased from Poland and it is out of stock until the end of May. I have asked if possible to purchase from another supplier and also for a date when the repairs can be made.

I am awaiting a response.

I have taken the Lion Seesaw on the toddler play area at the recreation ground out of use because both springs have completely broken and have ordered this repair to happen, hopefully, at the same time as the other repairs.

The Forty

Mowing of the footpaths around and through the wild area will begin as necessary with a volunteer and our maintenance person mowing alternate weeks.

The maintenance person will be replacing the bollards which have fallen and are rotten.

Dog Waste Bins

The additional dog waste bin has been installed on the verge on the other side of the main railway bridge off West End by the maintenance person. It has been well received.

Defibrillators

No update

Pavilion Car Park

Quotes from contractors.

	Description	Quote	+ VAT
Contractor A	Installation of a fully permeable shingle car park, using shingle grid system. French drains to help with percolation and new concrete edgings to finish against existing tarmac.	£61,466.40	£73,759.77
Contractor B	Works to be carried out in one visit. Moving, slewing or working around services to be extra. Muck away priced as inert. WAC testing to be done by others prior to works starting. Works area to be closed off during works. CBR tests by others in advance if required. All works priced on a remeasure. Site to be clear of cars for white lining.	£43,434.70 £1,138.83	£52,121.64 £1366.59
Contractor C	Awaiting quote		

Tree Risk Assessment Surveys.

I originally contacted two qualified Tree surgeons and four arboriculturists to obtain quotes for the tree risk assessment survey. I have listed below the responses I have received.

Quotes from contractors.

	Description	Cost	+ VAT
Contractor A	Carry out a tree survey and provide a report for trees in recreation ground (139), the Forty (2), St Mary's Churchyard (87), Ilges Lane site (4), Millenium Wood (80)	£3600.00	£4320.00
Contractor B	Carry out a tree survey and provide a report for trees in recreation ground (139), the Forty (2), St Mary's Churchyard (87), Ilges Lane site (4), Millenium Wood (80)	£1450.00	£1740.00
Contractor C	Carry out a tree survey and provide a report for trees in recreation ground (139), the Forty (2), St Mary's Churchyard (87), Ilges Lane site (4) Millenium Wood (80)	£1200.00 £200.00 approx	£1440.00 £240.00

I have researched and have spoken to arboriculturists for recommendations about the frequency of Tree Risk Assessment Surveys.

It seems that a frequency of 18 months or 28 months is the recommendation. This would mean the trees will be regularly surveyed alternately in full leaf and in winter dormancy.

If council can agree to a frequency for the surveys to be carried out it can be included in the full Tree Risk Assessment Plan.

TERMS OF REFERENCE
Station Working Group, Cholsey Parish Council

Document History

Version	Date	Details
1	17/04/2024	Approved at Annual Council meeting

1. Working Group remit

To investigate and pursue the initiation of improvements to Cholsey Station, including but not limited to improved platform accessibility.
To liaise and engage with key stakeholders as required.
To engage with residents, including conducting consultations as required.
To co-opt non-Councillor members to the Working Group whose presence would assist the Working Group.
To regularly report back and make recommendations to full Council as requested.

2. Appointment of Members

The Working Group will be comprised of at least three Councillor members, who are appointed by the full Council, with a quorum of two Councillor members. The Council will appoint one of the elected members to be the Working Group's Chair.

The Working group may co-opt non-Councillor members whose presence would assist the Working Group. Non-Councillor members shall meet the eligibility criteria to be a Councillor in the Parish of Cholsey.

The Working Group Chair may also invite appropriate experts and interested parties to Working Group meetings to advise the Working Group. Such invited participants will have the freedom to participate in the meeting but not to vote on decisions.

3. Duties and scope of responsibilities

- The Working Group Chair will be responsible for calling meetings and ensuring that meeting notes are kept.
- Councillor members of the Working Group will ensure that progress reports are made to full Council as requested.
- The Working Group has no power to authorise expenditure on behalf of the Council.
- The Working Group has no powers to alter or temporarily suspend this Terms of Reference document without full Council approval.
- All powers shall be exercised in accordance with the Standing Orders and other policies adopted by the Council.

4. Review

This Terms of Reference document was approved for use at the meeting of the Parish Council on INSERT DATE and shall be reviewed at least annually, or sooner should legislation dictate.

Signed by
Cllr Lis Nixon
Chair of Cholsey Parish Council

Payments Report, Cholsey Parish Council, April 17th 2024 meeting APPENDIX G

Signatures of authorising Councillors:

Payments made between meetings			
Play Inspection Co	Annual playground safety inspection	£297.00	Agreed on 13/03/2024 via email by Finance Committee
Allums of Oxon	50% of agreed allotment clearance	£887.50	Agreed on 13/03/2024 via email by Finance Committee
HCI data	Annual gov.uk renewal	£114.00	Agreed on 13/03/2024 via email by Finance Committee
OALC	Annual membership fees	£954.22	Agreed on 13/03/2024 via email by Finance Committee
J.Drewe	Ilges Lane allotment hedge coppicing	£1,740.00	Agreed on 13/03/2024 via email by Finance Committee
Gee Tee Bulb CO	CHEC spring bulbs	£46.48	Agreed by The Clerk
Ebay - CHEC expenses	CHEC tree stakes	£11.39	Agreed by The Clerk
Ebay - CHEC expenses	CHEC tree rabbit guards	£30.99	Agreed by The Clerk
Mileage	Maintenance Person	£18.40	Agreed by The Clerk
Fuel	For maintenance equipment	£67.24	Agreed by The Clerk
Cholsey Village CIC	Agreed wages donation	£2,600.00	Agreed at previous Parish Council meeting
Hazell & Jefferies	Allotment clearance skip hire	£1,044.00	Approved on 19/04/24 via email by Parish Council Chair
Castle Water	Burial Ground water	£1.87	Agreed by The Clerk
Castle Water	Burial Ground water	£10.24	Agreed by The Clerk
Cholsey Pavilion Trust	CHEC room hire	£30.00	Agreed by The Clerk
Colliers		£41.00	Agreed on 25/03/2024 via email by Finance Committee
Pavilion garden plants		£44.85	Agreed by The Clerk
Cantwell Hemmingway/Power Team	Monthly Payroll	£54.00	Agreed on 25/03/2024 via email by Finance Committee
Castle Water	Station Road allotment water	£65.27	Agreed by The Clerk
Castle Water	Ilges Lane allotment water	£70.50	Agreed by The Clerk
CHEC event expenses (Chiltern Conservation)		£61.60	Agreed on 28/03/2024 via email by Finance Committee
	TOTAL	**£8,190.55**	

Payments Report, Cholsey Parish Council, April 17th 2024 meeting APPENDIX G

Automatic payments			
Virgin Media	Telephone & broadband	£83.15	Inv VAT. £29.85 invoiced to Happy Hub for their charges.
Grundon	Burial Ground waste collection	£64.50	Inc VAT.
Nest	Staff Pensions	£132.32	
Staff salaries	Mar-24	£3,769.58	
Gap HR	Monthly HR support	£56.40	Inc VAT.
	TOTAL	**£4,105.95**	
Payments for agreement			
	TOTAL	**£0.00**	
Income received			
VAT return	Up to 30.12.2023	£4,623.76	
1st half of 2024/25 precept		£99,009.50	
	TOTAL	**£4,623.76**	
Income expected			
	Up to 31.03.24	£1,648.47	
	TOTAL	**£1,648.47**	