RACKENFORD AND CREACOMBE PARISH COUNCIL

Annual Meeting of the Parish will be held at Rackenford School, on Tuesday 3rd July 2018, starting at 7.30pm, followed by the Parish Council Annual Meeting. All councillors are summoned. Members of the public are welcome.

Parish Clerk: Karen Ward, 8 Peard Road, Tiverton, EX16 4LQ. Phone 01884 798711

AGENDA

1. **Apologies**

2. **Declaration of Interests**

3. **Open Forum**

4. **Minutes:** To sign, if approved, the minutes of the 1st May 2018 meeting.

5. **Report from District and County Councillor**

6. **The Common**
   a. Landscape Architect: Initial concept designs and updates

   b. Use of the Common for organised events:
      - to agree a hire agreement template
      - to discuss and agree principles of when the Common can be hired for organised events

   d. Hard court signage: To consider and approve new signage for the hard court

   e. Common/Children's Play Area: To consider any urgent repairs and maintenance

   f. Treatment of invasive species: To note treatment carried out to date and consider any future treatments required.

7. **Highways & Footpaths:**
   a. DCC consultation on proposed removal of Emergency SOS phones from the A361. Should the Council object to the removal the contributions, to consider to make any financial contribution towards their replacement and upkeep.

   b. Highways: General update and any issues to report

   c. Footpaths: Update and any repair or maintenance matters to report

8. **War Memorial**
   a. Location of War Memorial: following the accident, to discuss and agree the most appropriate location for the War Memorial

   d. Update on cleaning works to the War Memorial

   c. WW1 Centenary: To consider any events to mark the centenary of the end of the War

9. **Trinity Well:** Update on any repair works and consider longer term repair needs

10. **Noticeboard:** To consider replacement of the village notice board

11. Planning

a. Applications for consultation:

b. Applications awaiting NDDC decision
c. 64854: Reserved matters (appearance, landscaping, layout and scale) for erection of one replacement dwelling at Highfield Farm Rackenford – no objections
64824: Exension to dwelling at West Batsworthy Cottage Rackenford – objections submitted
64839: Prior approval for change of use agricultural building to one dwelling house at West Batsworthy Farm – no comments submitted

d. Notifications / decisions from NDDC

12. Finance 2018/19

a. Financial report: See budget monitoring statement

b. NALC Pay Award 2018/19 – To approve an inflationary increase of 2% in line with the NALC 2018 recommended pay scales.

c. Internal Audit report: To receive a verbal report on the recommendations from the 2017/18 internal audit report.

d. Payments to approve:
- K Ward / HMRC clerks wages £328.39
- K Ward expenses £14.92

13. General Data Protection Regulations: To consider and approve the new GDPR Policies including Privacy Policy, Data Breaches Policy, Subject Access Request Policy and Document Retention Policy.

14. Batsworthy Cross Wind Farm: Verbal update

15. Shop/School: Verbal updates

16. Correspondence:
Mobile library consultation

17. Matters of Urgency for noting only

18. Next Meeting: Tuesday 4th September 2018 at 7.30pm

Karen Ward (Clerk) Dated: 16th June 2018

RACKENFORD & CREACOMBE PARISH COUNCIL - 3 JULY 2018 BUDGET MONITORING

Balance as at 31st March 2018			**£30,246.85**	
Income	**Budget**		**Actual**	**Variance**
Parish Grant	£360.00		£322.78	-£37.22
Precept	£5,941.00		£2,970.50	-£2,970.50
Interest (N'wide account)			£0.00	£0.00
Other - VAT			£0.00	£0.00
Other grants and donations			£0.00	£0.00
Hard Court Rent	£1,640.00	-£1,240.00	£0.00	-£1,640.00
	£7,941.00	-£1,240.00	£3,293.28	-£4,647.72

Expenditure	**2018/19 Budget**	**Budget Transfers**	**Payments to Date**	**This Month's Payments**	**Budget Remaining**
Direct service costs					
Common Maintenance	£325.00	£725.00	£0.00		£1,050.00
Grass Mowing	£150.00		£0.00		£150.00
Playground Inspection	£90.00		£84.00		£6.00
Hard court maintenance	£200.00		£0.00		£200.00
Salt spreading / ploughing	£250.00	£840.00	£1,090.00		£0.00
Trinity Well	£250.00		£0.00		£250.00
Other costs					
Audit Fees	£250.00		£104.63		£145.37
Clerk Salary + HMRC	£1,300.00		£282.77	£328.39	£688.84
Clerk Expenses	£40.00		£4.94	£14.92	£20.14
IT equipment / exps	£60.00	£41.00	£40.83		£60.17
Insurance	£900.00		£559.03		£340.97
Other	£50.00		£0.00		£50.00
School Room Hire	£150.00		£0.00		£150.00
DALC,Parish online,CPRE, ICO	£200.00		£73.44		£126.56
Website	£120.00		£0.00		£120.00
Contingencies	£906.00		£0.00		£906.00
Defibrillator costs	£0.00		£0.00		£0.00
S.137 grants and other	£2,500.00	-£1,640.00	£200.00		£660.00
Total revenue spending	£7,741.00	-£34.00	£2,439.64	£343.31	£4,924.05
Movement to and from reserves					
Car Parking and Path					
Hard Court Maint		£400.00			
Playground Maint					
Common regeneration project					
Computer replacement		-£41.00			
Snow Warden		-£840.00			
P3					
Defibrillator	£200.00				
War memorial					
General reserves		-£725.00			
	£7,941.00	-£1,240.00	£2,439.64	£343.31	£4,924.05

VAT paid		£253.96	
Balance		**£30,846.53**	£343.31
Lloyds Balance as at 24/5/18		£23,867.39	
Nationwide Balance as at 31/12/17		£6,979.14	
Less u/c cheques / income banked			
	TOTAL	**£30,846.53**	
		£0.00	

Summary of current			
Car Parking and Path	£1,000.00	Common regeneration project ph 1	£416.00
Hard Court	£10,053.56	Common regeneration project ph 2-4	6,000.00
Soft Play Area	£1,879.39	Computer Replacement	£944.00
P3	£837.34	Snow Warden	£760.00
Defibrillator	£800.00	War Memorial	£500.00
		Rackenford PC	**£7,656.24**
			£30,846.53

RACKENFORD AND CREACOMBE PARISH COUNCIL

Meeting 3 JULY 2018

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 Rackenford and Creacombe Parish Council which is the data controller for your data.

3. What personal is collected or held?

- 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.
- Where you pay for activities such as or hire of the hard court, 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 mental and physical health, details of injuries, medication/treatment received
- Information from other sources e.g.
  - From other Councils
  - Publicly accessible sources such as the NDDC planning website
- Nature of any outbound communications with website users
  - Email
  - Telephone (voice)

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
- 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.

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.

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.

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.

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.

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 may be accessed from overseas].

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

Changes to this policy
We keep this Privacy Policy under regular review and we will place any updates on http://www.rackenford-devon.co.uk/parish-council/rackenford-parish-council.php. This Policy was last updated in **June 2018**.

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: Rackenford and Creacombe Parish Council, 8 Peard Road, Tiverton, EX16 4LQ
Email: clerk@halberton.org

Data Breach Policy

Nature of likely breaches / loss of data

- Theft of council laptop including access to payroll information, emails, all council business
- Employee personal data breached when submitting to HMRC or NEST
- Accidental forwarding / sending emails to wrong person
- Sending emails without personal information redacted / deleted
- Non-council members accessing council emails
- Lack of back up procedures

The breach response plan
If a breach has occurred, or may have occurred, the Chairman, Vice Chairman and Clerk should be notified immediately.

The Chairman, Vice Chairman and Clerk will agree what steps should be taken in accordance with the data breach checklist below, which may include logging the breach, informing those whose data has been breached, mitigating actions, informing all members, reporting to ICO, implementing lessons learned

Data Breaches checklist

Mitigating / preventative actions to be reviewed regularly

- Understanding what data you hold (and what you shouldn't hold)
- Making sure data appropriately classified
- Having, and applying, data destruction policies
- Understanding what data is encrypted, how it is encrypted, and when it may be unencrypted on your systems
- Regularly check you are complying with your retention policy to ensure you are storing only the data you should be
- Having appropriate additional protection for sensitive data
- Having data loss prevention or similar tools
- Understand your logs, how long you retain them for and what they can (or cannot) tell you
- Having appropriate logging of staff/ councillor access to data
- Understand the basic IT do's and don'ts of responding to data breaches
- Have an asset inventory to help you identify potentially compromised devices, where those devices are and in whose possession
- Understand how data flows in your council, in practice
- Cover for cyber breach insurance, or other insurance which may cover a data breach
- Understand the process for (a) notifying breaches and (b) obtaining consent for actions from insurers
- Emergency contact details for your brokers
- Access to PR capability experienced in dealing with data breaches
- Template pro-active and re-active press statements

In the event of a data breach:

Data subjects

- Understand when you should consider notifying data subjects
- Understand the contractual and legal rights of data subjects
- Quickly prepare appropriately worded notifications to data subjects
- Understand the potential harm to data subjects of loss of the different types of data that you hold
- Ability to appropriately triage and deal with a breach
- Councillors and staff appropriately trained as to how to deal with data subjects in a breach scenario

Legal issues

- Process for maintaining legal privilege and confidentiality
- Pausing document destruction processes
- Evidence gathering capability so you can collect information about the breach
- Appoint specialist external lawyers who can manage the investigation and give legal advice
- Process for managing and logging steps taken in the investigation
- Understand your contractual rights and obligations with third parties
- Identifying third parties you may need to notify
- Having appropriate contractual rights to be notified of breaches by third parties
- Contact the Information Commissioners Office ("ICO") and with law enforcement who you can involve quickly if necessary
- If holding credit/ debit card data, notify your payment processor
- Advice on the legal options available to quickly gather evidence from third parties
- Understand potential liabilities to third parties
- Gather information about the breach including taking statements from staff members or councillors who might have seen unusual activity
- Understand when you should consider notifying data subjects and / or regulators

Forensic IT

- Access to qualified forensic IT capability, either internally or externally
- Secure and isolate potentially compromised devices and data, without destroying evidence
- Quickly ensure physical security of premises

Public Relations

- Actively monitor social media and other media after a breach

Cybersecurity checklist

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

- Council member with responsibility for cyber security
- Clear responsibility for cyber security, with clear reporting lines and decision-making authority
- Allocate sufficient budget to cyber security
- Subscribe to cyber security updates so that you are aware of threats

People

- Appropriate mechanisms for staff and councillors to be able to report suspicious emails quickly and effectively
- Train staff and councillors on cyber security regularly
- Councillors and staff undertake reviews to ensure that they understand cyber security risks
- Have proper processes for when staff or councillors join or leave the council, and are they applied in practice?
- Staff and councillors understand the risks of using public wifi
- Conduct appropriate checks on new staff and councillors to understand if they are a potential security risk

Hardware, data, encryption and technology

- Backup personal data encrypted
- Have appropriate mechanisms for securely sending files
- List of servers, and individuals who are responsible for ensuring that they are up to date
- Appropriate firewalls and intrusion detection software
- Wireless networks appropriately secured?
- Regularly check the operating systems, data and software against a 'good known state'

baseline
- Review unsuccessful attacks and probes / scans
- Inventory (or list of) hardware and software you use
- Appropriately limit access to data on a 'need to know' basis
- Back-up personal data on a regular basis
- Apply regular IT updates to your computer hardware and software
- Ensure that staff and councillors have anti-virus software loaded and active on their devices at all times
- Have appropriate policies regarding use of external hard drives or USB drives
- Conduct regular penetration tests and / or red teaming, with appropriate analysis of results

Third parties
- Understand risks arising from third party service providers
- Undertake due diligence before engaging third party service providers
- Assess third parties for cyber security or data protection risks
- Have obligations in your contracts with third parties requiring them to take steps to keep data secure
- If using cloud storage, do you have contractual rights to be notified quickly of potential security issues

Remote access/BYOD
- Require multifactor authentication where appropriate
- If allowing remote access having the right software and controls in place to ensure it is secure
- Have policies to secure mobile devices
- Data encrypted on mobile devices
- Mobile devices be remotely wiped
- If using BYOD, do you apply restrictions to maintain security

User accounts / passwords
- Require unique user accounts
- Require multifactor authentication where appropriate
- Restrict administrator accounts to the minimum necessary
- Require strong, hard to guess, passwords
- Automatically prevent use of common passwords

Glossary
"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, which restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.
"**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.
"**Cyber security**" is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
"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.
"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).
"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.
"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.
"**Red teaming**" using consults to test your physical and systems security.
"**Remote access policy**" is a document which outlines and defines acceptable methods of remotely connecting to the internal network.
"Remote access" is the ability to get access to a computer or a network from a remote distance.
"Wifi" a facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

Subject Access Requests Policy

- On receipt of a subject access request **forward** it immediately to Clerk, and inform the Chairman and Vice Chairman.
- Correctly **identify** whether a request has been made under the Data Protection legislation

  Ensure the 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 appropriate person (staff, councillor or volunteer) who is given the task of of locating information and supplying personal data relating to a SAR must make a full exhaustive **search** of the records to which they have access. The information should be forwarded to the Clerk.

  Depending on the degree to which personal data is organised and structured, searches will include 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.
- All the personal data that has been requested must be **provided** unless an exemption can be applied.

  Personal data will not be withheld because it may be misunderstood; instead, an explanation will be provided with the personal data and it will be provided in an “intelligible form”. 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. Exempt personal data will be redacted from the released documents with an explanation why that personal data is being withheld.
- A **response** must be made within one calendar month after accepting the request as valid.
- Subject Access Requests are **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.
- Councillors must ensure that the staff they manage are **aware** of and follow this guidance.
- Where a requestor is not satisfied with a response to a SAR, the council must manage this as a **complaint**. 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.

Sample letters for subject access requests

All letters must include the following information
- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses;
- where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
- 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;
- the right to lodge a complaint with the Information Commissioners Office (“ICO”);
- if the data has not been collected from the data subject: the source of such data;
- 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.

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

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

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

Document Retention Policy

Document	Retention period
Minutes (and agendas if applicable)	Indefinite
Policies	Current policies only held
Scale of fees and charges	6 years + current year
Financial accounts including receipts and payments	6 years + current year
Bank statements	Last completed audit year
Paying in books	Last completed audit year
Cheque book stubs	Last completed audit year
Quotations and tenders	6 years + current year
Invoices, expenses and cheques	6 years + current year
VAT records	6 years + current year
Timesheets	Last completed audit year
Payroll	12 years + current
Insurance policies	Indefinite
Certificate for insurance against liability for employees	40 years from date of renewal
Investments	Indefinite
Title deeds, leases, agreements, contracts	Indefinite
Trust deeds	Indefinite
Members allowances register	6 years + current
Planning matters	While current only
Information from other bodies e.g. DALC	While useful and relevant only
Magazines and journals produced	Where required under Legal Deposit Libraries Act 2003, copies will be sent to the British Library Board
Correspondence	Retained while relevant only.
Staff documentation	While valid only, subject to being required for the purposes of taxation, references, pensions etc.
Local/historical information	Retained or lent to the Devon Archives where considered important
Retention of documents for legal purposes	As set out in the Limitations Act 1980