Acceptable Use Agreement

1. Teignbridge District Council provides iPads to support all Councillors in the course of their duties as an elected member of the Council. This agreement sets out the details of the ICT equipment and services that are provided to all Councillors for the duration of their term of office.

2. This agreement must be read in conjunction with other relevant ICT provisions including:

   a) The Council's Acceptable Use Policy, Data Protection Policy and Safe Emailing guidance
   b) The requirements of the Data Protection Act and GDPR in regard to Councillors' personal responsibilities and liability as a Data Controller and Data Processor and
   c) Relevant provisions within the Councillors' Code of Conduct.

3. The objectives of Councillors' ICT provision are:

   (a) to maximise the effectiveness of Councillors in their role; and
   (b) to enhance communications between Councillors, officers, partners and members of the public

4. Electronic communication is an essential part of a Councillor's role. It will be used to inform them of important information such as dates of meetings, briefings, training events and notification of agendas and minutes along with e-mails from the public and officers.

5. Councillors are expected to check their Council e-mail account on a regular basis to ensure awareness of all relevant information relating to their role and any executive and committee responsibilities.

6. In order to ensure the security, confidentiality and management of information and personal data, Councillors must not use their private email addresses for council business. The forwarding of emails from Councillors' TDC accounts to their personal email is prohibited.

7. With the increasing use and access to mobile computing devices and in line with the Council's Digital Strategy, there will be an expectation that all Councillors will view committee agendas and reports online rather than require printed hard copies.

8. The Democratic Services Team Leader will make arrangements to assist any Councillor requiring reasonable adjustments to this policy in line with the Council's commitment to inclusivity and in compliance with the Equality Act 2010. Any Councillor wishing to discuss this should contact the Democratic Services Manager. All conversations will be treated in the strictest confidence.

9. Councillors must sign confirmation that they have received their device and accept this agreement as terms of its use.

10. In addition, Councillors may access their Council e-mail account via a compatible, personal smartphone subject to the installation of the Council's Mobile Device Management software on the device. This enforces specific security controls such as access to the device, and remote wipe in the event of loss or theft. The Council will pay for the relevant software licence for this access for the duration of the Councillor's term of office but not for the device or airtime contract.

11. The Strata Service Desk will assist Councillors with the use of Council supplied equipment (currently iPads) and provide general advice associated with the personal equipment connecting to the email service on a reasonable endeavours basis. It is the responsibility of the Councillor to ensure they have appropriate support services and contracts to manage their personal devices for incident and fault resolution.

12. Councillors are expected to meet connectivity costs of devices such as broadband and Wifi.

13. Councillors will be responsible for the safekeeping of any Council equipment issued to them and expected to treat it with appropriate care to avoid it being damaged, lost or stolen.

14. The loss or theft of any device with access to Council data, whether Council owned or personal, must be reported immediately to the Strata Service Desk to allow the earliest opportunity to assess the information risk, wipe the device where possible, and notify the Information Commissioner's Office within the statutory 72-hour deadline under the GDPR, where necessary. The Council will contact the ICO should a notifiable breach occur.

15. Inappropriate use of the equipment or services or breaches of the relevant associated policies may bring the Council into disrepute and result in action being taken under the Councillors' Code of Conduct.

16. You must not, nor attempt to, bypass any security measures in place for the protection of TDC's networks, systems, data and information.

17. For personal devices you must ensure that access to them is protected by suitable access mechanisms, either a pin code (minimum 6 length), password or biometric (usually finger print but also now face recognition). Advice can be provided from Strata.

18. You are solely responsible for the security of the ICT systems you are authorised to use along with any system passwords. All passwords must remain confidential and must not be shared with anyone else.

19. You must not use a personal email account for TDC business. You must not forward TDC data or documents to your personal email account(s). You must not use a TDC email account for personal purposes.

20. You must not access or distribute, nor attempt to access or distribute, illegal material or any material which may bring the District Council into disrepute.

21. You must not download or install any software, applications (Apps), or other forms of executable files from the internet, personal, or third-party storage locations onto Council provided devices, except from agreed sources, currently the 'Airwatch Catalog'

22. The iPads should be returned to Democratic Services within five days after the last day of office.

Declaration

I confirm that, as an authorised user of the District Council's systems, I have read and understood the ***Acceptable Use Agreement.***

Name:

_____

Ward:

_____

Signature:

_____

Date:

_____