

## **LEDBURY TOWN COUNCIL**

### **INFORMATION, COMMUNICATION & TECHNOLOGY (ICT) POLICY**

Ledbury Town Council recognises the importance of e-mail, the internet and telephone facilities in the successful achievement of its aims and objectives.

All staff are actively encouraged to use such facilities in accordance with the procedures laid down.

The Council is fully aware of the need to safely back-up all data held on its computer systems which is covered by a remote external programme that operates every 24-hours. In cases when this is not possible all users will ensure that all data is saved on at least a weekly basis to memory sticks or similar external devices and stored remotely. All back-up processes will be carried out in accordance with the requirement of GDPR Regulations.

Date adopted by the Council – 30 July 2020

Date for Review – July 2022

## **Draft Information, Communications and Technology Procedure**

All staff must be authorised by the Town Clerk to use any IT facilities provided by the Council and in the case of the Town Clerk authorisation will be given by Council.

All staff are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services. Any accidental damage or disruption must be reported to line managers as soon as possible after the incident has occurred.

All employees are responsible for any IT activity which is initiated under their user name:-

- Passwords and account details must not be divulged and computers must be locked when employees are away from their desks
- Password protected screen savers should always be used
- Passwords should be changed regularly (at least every 6-months) and should be literal and numeric with a minimum of six characters

All employees must comply with all the relevant legislation covering IT use, namely:-

- Data Protection Act 1998, GDPR Regulations 2018 and Freedom of Information Act 2000

Any information which the Council holds is potentially disclosable to a requester under these Acts, which includes emails.

Under the Computer Misuse Act 1990 it is an offence to try and access any computer system for which authorisation has not been given;

Under the Copyright Design and Patents Act 1998 it is an offence to copy software without the permission of the owner of the copyright;

Under the Deformation Act 1996 it is an offence to publish untrue statements which adversely affect the reputation of a person or groups of persons

Under the Terrorism Act 2026 it is a criminal offence to encourage terrorism and/or disseminate terrorist publications

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows any organisation to monitor or record communications (telephone, internet, email and fax) for defined business related purposes

### **Use of Council Telephone System**

Desk or fixed telephones are provided to all office and employees to enable them to perform their duties. The provision of a mobile phone will be agreed if a business case is approved by the Council for which network charges and business calls will be paid for by the Council

- Internal phones must not be diverted to mobile phones unless specifically detailed in other policies
- Employees positions and telephone numbers will be listed in the Councils directories

Employees may use their desk/fixed telephones for personal use but this should be during their break periods

Employees may use their own mobile phones if necessary, again this usage should be restricted to break periods,

### Use of E-mail

E-mails sent or received form part of official records of the Council, they are not private property. E-mails may be disclosed under the Freedom of Information Act, as part of legal proceedings (e.g. tribunals) and as part of disciplinary proceedings.

Employees are responsible for all actions relating to their e-mail accounts/user name and must ensure that no other person has access to their account without the permission or knowledge of the Clerk or Deputy Clerk.

When using the Council's e-mail employees **must**:-

- Correctly maintain their own e-mail folders and delete all unwanted mail on a regular basis
- Not use e-mail for the creation, retention or distribution of disruptive or offensive messages, images, materials or software that includes offensive or abusive comments about ethnicity, nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Employees who receive e-mails with this content must report the matter to their line manager.
- Not send e-mail messages that might be reasonably considered by the recipients as bullying, harassing, abusive, malicious, discriminatory, defamatory and libellous or containing illegal or offensive material or foul language
- Not upload, download, use, retain, distribute or disseminate any images text materials or software which might reasonably be considered indecent, obscene, pornographic or illegal
- Not engage in any activity that is outside the scope of normal work related duties
- Not send chain-letters of joke e-mails

Personal use of the Council's e-mail is NOT permitted without the prior permission of your line manager and should be restricted to the employees break periods if permitted.

## Use of the Internet

Use of the internet by employees is encouraged where such use is consistent with their work and with the goals and objectives of the Council in mind reasonable personal use is permissible, but this is to be restricted to break periods.

Employees **must not**:-

- Participate in any on-line activity that would bring the Council into disrepute
- Visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography) obscene matter, race hate material, gambling and illegal drugs
- Knowingly introduce any form of computer virus into the Council's computer network
- Download commercial software or any copyright material belonging to third parties unless agreed
- Use the internet for personal financial gain
- Use gambling or on-line auction sites or social networking sites such as Facebook, LinkedIn, You-Tube, Twitter, MySpace etc. unless it is for the purpose of carrying out their duties

**Abuse of these procedures could lead to disciplinary action being taken.**

## Use of Social Media Sites

Personal use of social media sites in working hours is NOT permitted and when using social media sites employees should be mindful of the following points:-

- Bringing the Council into Disrepute – if an employee names their workplace on a social media site then they should not enter into any activities whereby their actions could bring the Council in disrepute. These would include discussing Council business in an open forum, referring to Councillors or colleagues in a negative manner etc.
- Bullying or Harassment of Colleagues – All employees should show respect for their colleagues and councillors at all times and should not bully or harass them in any way. This also applies to social media websites and therefore employees should not make derogative remarks which could be deemed as bullying or harassment about their colleagues or councillors at any time on any social media sites.
- Libel Content – Employees should not publish in print (including pictures) an untruth about another which will do harm to that person's reputation by tending to bring the target into ridicule, hatred, scorn or contempt of others, i.e. print libel content

**Abuse of the above procedures will lead to a disciplinary investigation.**

Date adopted by the Council –

Date for Review –