**Information Security Tips for**

**Harborough Energy (HE) & Harborough Solar One (HS1)**

***A Common Sense Guide to Good Practice Regarding Data Protection (v1.2/DJR/Issued)***

**1. Who does this apply to?**

**EVERYONE -** eg Directors, Committee Members, Officers, Consultants, Contractors, Volunteers and anyone else authorised to see and use HE / HS1 related information and systems.

**2. Why should I bother?**

**IT’S THE LAW** – we have a nominated Director accountable for Data Protection (currently David Robbins) but anyone working for us or with us needs to adhere to the current Data Protection Act (<https://ico.org.uk/for-organisations/guide-to-data-protection/>) and the new General Data Protection Regulations (<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>).

**3. What do I need to know and do?**

**USE COMMON SENSE** - following simple practical steps to ensure that you and HE / HS1 are treating personal information correctly, processing it as agreed, keeping it secure and up to date then disposing of it safely, when no longer relevant. These include simple measures like:

* Ensuring informed consent has been given to keep and use personal information
* Password protecting and saving as encrypted, where available (eg Excel, Word)
* Using strong passwords and keeping them secure (see 'Top 5 Tips' below)
* Not giving out or sharing logon credentials (such as, username or password)
* Blind copying rather than emailing to all (eg investor communications)
* Having appropriate IT security in place to prevent personal information being accidentally or deliberately compromised (eg up to date antivirus and internet protection; encrypted memory sticks / flash drives, regular data backups, etc)

Please think carefully before requesting, accessing, processing or sharing any personal information on behalf of HE or HS1 - **if you are unsure what to do** then please contact us on HarboroughEnergy@gmail.com ***before*** taking any action.

This short document covers **some of the basics** and provides **useful links** to further guidance from the Information Commissioner's Office (ICO). *Failure to comply can be fined up £500k.*

**4. What are the 'Eight Principles'?**

The **Data Protection Act 1998** became law in March 2000. It was designed to protect personal information about living individuals, and sets standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data. Organisations **must** comply with the **eight enforceable principles** of good information handling practice. Personal data must be:

* Processed fairly and lawfully
* Obtained only for one or more specific and lawful purposes
* Adequate, relevant and not excessive in relation to the purpose(s) for which they are processed
* Accurate and where necessary kept up to date
* Not kept for longer than necessary
* Processed in accordance with the individual’s rights
* Protected by appropriate security (practical and organisational)
* Not transferred to countries outside the European Economic Area, unless there is adequate protection

**5. What is the 'GDPR' and how should we be preparing for it?**

The **General Data Protection Regulation (GDPR)** is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal data from **25 May 2018**.

The ICO has produced a useful 12 step checklist to ensure organisations are prepared for the GDPR: <https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf>

***HE / HS1 is ensuring it is ready and is updating its procedures and guidance accordingly. Our data protection policy will include document referencing and version control along with a central register of key data held, privacy notices and retention periods, where it is stored and who has access (including our banking).***

The ICO also provides specific help for not-for-profit, charitable and voluntary organisations (like HE / HS1) to comply with our responsibilities to information rights, such as their **Top 5 Tips**:

* **Tell people what you are doing with their data -** People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.
* **Make sure your staff are adequately trained** - New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.
* **Use strong passwords -** There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lowercase letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.
* **Encrypt all portable devices -** Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.
* **Only keep people’s information for as long as necessary -** Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

**6. Where can I find further information?**

More details including the useful **GDPR FAQs document** are provided at: <https://ico.org.uk/for-organisations/charity/>

An excellent **Practical guide to IT Security** for small businesses is available from the ICO at: <https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf>