Crouch Harbour Authority's Information Security and UK General Data Protection Regulation (GDPR) Policy

1. Purpose of this policy

This policy sets out Crouch Harbour Authority's guidelines on how to keep information secure at work.

2. Scope of the policy

This policy applies to all employees including those who work part-time or on fixed-term contracts.

3. Roles and responsibilities

At Crouch Harbour Authority:

- senior managers have overall responsibility for this policy
- line managers are responsible for ensuring their team complies with this policy
- all employees are responsible for following the policy and reporting any breaches to the Crouch Harbour Authority Chairman

Please contact the Senior Manager if you have any questions about this policy, email info@crouchharbour.org.uk.

4. Compliance with UK GDPR

The UK GDPR requires all businesses to use technical and organisational processes to ensure information security. However, the UK GDPR does not set out how to do this.

Crouch Harbour Authority will set out in this policy how it will achieve information security in line with UK GDPR requirements.

5. Guidelines for all information

Crouch Harbour Authority will:

- identify information which needs to be treated as personal or special category data
- apply the data protection principles which are outlined in the UK GDPR
- process personal data in a lawful way

However, all information, whether it is physical or digital must be:

- treated with great importance
- protected from:
    - loss
    - theft
    - misuse
    - inappropriate access or disclosure
- handled in line with Crouch Harbour Authority's other policies on:
    - data protection

6. Access to premises

Access to all Crouch Harbour Authority premises by non-employees, such as visitors and contractors, must be logged and monitored. They must:

- be accompanied or supervised by an employee
- not be left alone or put in situations where they have unsupervised access to company information

6.1. Meetings

Visitor meetings must take place in a designated meeting room. If this is not possible, the meeting should take place in another room which has no access to company information. The only exception to this is where information is required for the purpose of the meeting.

6.2. Admission to buildings

Only employees will have keys and access codes to the premises. They must be:

- kept safe and secure

- used for their own access only
- not given to any third party

7. Information in physical form

All physical documents which contain company information must be kept secure. This means it must be in lockable storage when it's not in use, such as:

- when employees are away from their desks
- at the end of the day

Only employees who need access to the information should have the keys or combinations to access the information in the storage area.

Keys and combinations should not be left lying around. Keys should not be left in keyholes of the storage units.

8. Information in digital form

Crouch Harbour Authority has various protections in place to keep its digital information safe.

8.1. Policies

Crouch Harbour Authority have the following policies which relate to keeping digital data secure and should be read alongside this policy:

- data protection policy

8.2. Cyber security measures

Cyber security is the measures taken to protect a business' systems from threats posed by cyber criminals such as hacking, phishing and malware. Measures Crouch Harbour Authority include:

- staff awareness on cybersecurity
- anti-virus software
- secure wifi connection
- rules on ensuring strong passwords
- backing up data

- company phones mobile device management

8.3. IT and software support

The Computer Centre's IT department will provide employees with IT support to help keep information safe.

This includes:

- assistance with user accounts including:
    - creating, modifying, deleting and reviewing accounts
    - technical controls
    - preventing unauthorised access
- help employees understand how information is backed up and accessed if needed
- setting up employee devices including personal devices for work purposes (if they are permitted)
- implementing and maintaining:
    - firewalls
    - anti-virus software
    - patch management

Harbour Systems Ltd are a data processor and provide hosting and support for eHarbour software, they provide employees with IT support to help keep information safe.

This includes:

- assistance with user accounts including:
    - creating, modifying, deleting and reviewing accounts
    - technical controls
    - preventing unauthorised access
- help employees understand how information is backed up and accessed if needed
- setting up employee devices including personal devices for work purposes (if they are permitted)
- implementing and maintaining:
    - firewalls
    - anti-virus software
    - patch management

8.4. Measures employees will take

Crouch Harbour Authority will make sure employees contribute to keeping digital information secure by:

- locking their systems when they are not in use
- cyber and security awareness
- only using devices provided by or approved by Crouch Harbour Authority
- regularly changing passwords
- being careful and vigilant when it comes to potential cyber attacks
- referring all potential cyber security issues to IT

9. Communication

9.1. Verbal communication

Trustees and employees must take care when discussing Crouch Harbour Authority's business in and out of the office. They should not discuss Crouch Harbour Authority business:

- with those who are not colleagues
- in public places

Strict confidentiality must always be maintained.

9.2. Written communication

Employees must:

- verify all postal and email addresses before sending communication
- where appropriate, encrypt information which is either personal or sensitive personal data
- ensure communication is being sent to the correct recipient. Particular care should be taken with email addresses where auto-complete features may have insert incorrect addresses
- when sending emails to multiple recipients, use 'bcc' rather than 'cc' unless all recipients need to collaborate on the subject matter

10. Transfer of information

10.1. Taking information home

If an employee or trustee needs to take Crouch Harbour Authority's files or information home, they need to:

- maintain confidentiality
- keep the information secure by:
    - ensuring devices are encrypted and locked away when not being used
    - not transporting paper copy in see-through or other unsecured bags or cases
    - not accessing it in public
    - not leaving it unattended. For example, in a car when they are not in the car

10.2. Use of personal accounts

Crouch Harbour Authority's employees are not permitted to use personal email addresses or cloud storage services for work purposes. This is because they don't offer the same security as Crouch Harbour Authority's systems.

10.3. Working from home and remote working

When employees work from home and/or remotely the data protection principle most at risk is that data needs to be:

- processed in a manner that ensures its security
- protected against unauthorised or unlawful processing
- protected against accidental loss, destruction or damage

To help employees keep information secure, Crouch Harbour Authority will:

- circulate guidance on working away from the office and the associated information security risks
- make sure employees only use secure networks and wifi connections
- make sure all devices used have appropriate and up to date anti-virus and security software
- install multi-factor authentication
- encourage employees to be paperless when working away from the office
- remind staff to use unique passwords and not write them down

- invest in technology and software to improve information security and minimise risks
- make sure employees have adequate support in the event of issues

There are some additional things employees can do to ensure information security. They must:

- review Crouch Harbour Authority's's relevant policies and guidance on information security
- create a specific workspace and make sure it's secure
- turn off smart speaker devices while working
- not leave documents unattended
- tidy their workspace and lock away anything work-related at the end of the day. This includes:
    - devices
    - papers
    - all other information
- not put documents that contain personal data or confidential information in household rubbish or recycling
- be extra vigilant to fraudsters impersonating companies associated with Crouch Harbour Authority
- not open or reply to spam or phishing emails
- ask questions if they are unsure of what to do
- report any problems or potential breaches immediately

This list is not exhaustive.

10.4. Transferring information to third parties

Crouch Harbour Authority employees can only transfer information to third parties if:

- there is an agreement in place
- checks have been done to ensure they have appropriate data protection and information security measures in place
- the information is being sent in accordance with Crouch Harbour Authority's procedures

Crouch Harbour Authority must also consider if a third party would be considered a data processor under the UK GDPR.

11. Information and data breaches

As part of their responsibilities for helping us implement this policy, all employees, trustees, contractors and associated third parties must report potential breaches immediately.

This includes any incidents that involve:

- the sharing of personal data, whether accidental or deliberate, with parties who are not authorised to view it
- the loss or theft of a device that contains, or grants access to information held by Crouch Harbour Authority
- attempts by anyone to access Crouch Harbour Authority information or personal data held by Crouch Harbour Authority by hacking or bypassing IT security measures
- the unauthorised alteration or deletion of Crouch Harbour Authority information or personal data held by Crouch Harbour Authority

Potential breaches should be reported to info@crouchharbour.org.uk.

In cases where we believe a breach may pose a risk to someone's rights or freedoms, we will report it to the ICO. We will do this without undue delay and certainly within 72 hours of the issue being raised with us.

Not every risk will need to be reported to individuals concerned. We will only inform the ICO and relevant individuals where this is a high risk to people's rights and freedoms. This is so we do not cause individuals unnecessary anxiety.

If an employee's actions lead to a breach, whether this was deliberate or accidental, they may face disciplinary action. We will take this action in line with our disciplinary procedure, which can be found in the CHA Staff Handbook.

If we consider an employee's behaviour to be gross misconduct, this will usually result in dismissal without:

- warning
- a notice period
- payment in lieu of notice

Document reviewed 17/07/2025