SURREY HEATH BOROUGH COUNCIL

EMAIL SECURITY POLICY

March 2024

Surrey Heath Borough Council
Knoll Road, Camberley GU15 3HD
Data.protection@surreyheath.gov.uk

Contents

1. Introduction

Email is one of the most widely used business tools, utilised by all staff. It is an effective communication tool with large amounts of information shared on a daily basis. However, due to the nature, volume and format of emails, it is easy to make mistakes and therefore incorrect use of information sharing via email is one of the biggest threats to the security of the Councils information.

The Council are committed to making the best use of technology and continuously improve our information security. The key purpose of the Email Security Policy is to provide awareness and guidelines for all staff on the correct and safest use of email.

2. Definitions

Personal Data - 'Personal data' under the Data Protection legislation is information about a living individual who can be identified from the information. The information can be factual information (e.g. names and addresses) or expressions of opinion or intentions about an individual. Other examples of personal data include location of data, online identifiers (IP addresses and mobile devices ID's and photographs).

Phishing – Phishing is the use of bogus email and websites to trick an email user into supplying confidential and personal information or passwords.

Spamming – Spam is unsolicited commercial email, the electronic equivalent of the junk mail that comes through your letterbox.

Data Loss Shield (DLS) – Is a tool attached to outlook that set rules and policies to determine which files and data are considered confidential or sensitive and then protects those files.

Swift codes – Is a number that identifies bank and finance institutions

3. Scope

The Email Security Policy will apply to all employees (including fixed term, casuals, agency staff, contractors and work experience students, volunteers as well as permanent staff) employed on Council business, including those working with partner organisations and Councillors. This policy should be read in conjunction with the following policies and all other relevant policies will apply:

- Information Security Policy
- Data Protection Policy
- Email Management Guidance
- Box training tips on Warbler
- Disciplinary Policy and Procedures
- Code of Conduct for Officers
- Records Management Policy

The Council reserves the right to conduct investigations where a breach of the Email Security Policy is suspected. Breach of this policy may be dealt with under the council's disciplinary policy. Serious cases may be treated as gross misconduct leading to dismissal.

4. Principle and aims

4.1 The Council recognises that email is an effective communication mechanism. This policy is not intended to restrict Council email users from using email, but to make them aware of the risks they could potentially face with how they use email and share information.

4.2 To ensure that when email is used to communicate with the public, stakeholders and partners by all SHBC staff in the performance of their duties, that it is done so in accordance with the applicable SHBC Policies.

4.3 To ensure that any SHBC communication through email meets legislative and legal requirements.

4.4 To ensure that all Council email users are aware of the capabilities of monitoring and Data Loss Shield within MS Outlook and how the Councils is using the tools.

5. Accountability and responsibility

5.1 Head of Service, Strategic Directors and WMT

It is the responsibility of Heads of Service, Strategic Directors and WMT Managers to ensure that all staff are aware and adhere to the contents of this policy.

Where a breach of this policy is identified Head of Service, Strategic Directors and/or WMT may be asked to assist with any HR investigation.

5.2 Information Governance (IG) and ICT

The IG and ICT Department will monitor the use of the email system via the Data Loss Shield tool and Barracuda archive system. All Email stored may be inspected without notice to the staff member. Monitoring will be done where there is a business requirement or where there is a suspected breach or misuse of email. Some of the most likely reasons for monitoring email are:

- Preventing or detecting misuse
- Preventing or detecting crime
- Making sure email is operating properly
- Checking the quality of service
- In response to an Information Rights request i.e. Freedom Of Information, Subject Access Rights

The ICT & IG Departments will notify the respective Line Manager and Human Resources Department of any suspected breaches of this policy.

5.3 All Council email users

It is the responsibility of all users of Council email to comply with this policy and report any information incidents or near misses including breach of this policy to their line manager and/or Information Governance Manager.

Council email users should be aware that they neither own the documents that they or their colleagues create, nor have intellectual property rights therein.

6. Email content

6.1 The privacy and confidentiality of messages sent via email cannot always be guaranteed. It is the responsibility of all users of Council email to exercise their judgement about the appropriateness of using email when dealing with sensitive subjects or sharing personal or confidential data.

6.2 When sharing personal identifiable information by email, only ever share the minimal amount of information required, you should only send personal identifiable information where it is completely necessary and the correct security, appropriate to the recipient and the information that is being sent, is applied;

If you have satisfied that you are in email conversation with the subject matter and the sharing of their personal data is required, this is done with implied consent and therefore sharing of information via email is acceptable.

If you are required to share personal identifiable information with a third party and not the subject matter, additional security may need to be applied if the email is not secure, more information can be found in section 8 of this policy.

6.2.1 Examples of personal identifiable information include, but are not limited to;

- Common identifiers such as; name, address, email address
- Identification numbers such as; Passport Numbers, National Insurance Numbers (NINO) and NHS Numbers

- Online identifiers including; Council Tax number and other reference numbers

6.3 Credit/Debit card numbers, IBAN numbers and swift codes must never be written down or transmitted by email, when processing a 'customer not present' card transaction, an employee may only enter the card information directly into the Surrey Heath payment form as the payee provides the information.

6.4 Emails must be professional, courteous and use respectful terminology. It is recognised that emails have no 'tone of voice' and therefore care should be taken to ensure that they do not appear angry, defensive or rude. Training and guidance can be given to staff to help them write professional emails as required.

6.5 Salutations, signatures and 'out of office' on emails must follow organisational templates provided.

6.6 As a Local Authority copies of all emails can be requested under the Freedom of Information (FOI) Act. There are exemptions to withhold information within the FOI Act, however there is not one which covers causing embarrassment to the Council.

6.7 Council email users are advised that all emails sent externally from the Council automatically have a disclaimer at the footer of the email to protect the Council from information being disclosed to unauthorised personnel, however, there is no guarantee that this will protect individual personnel from potential legal action if emails sent include unsupported allegations, sensitive or inappropriate information.

7. Email access

7.1 Every user of Council email is responsible for ensuring that where possible their Council email account is kept secure and not inappropriately used. You should not allow anyone else to use your

Council email account and should never share your password or multi-factor keys with anyone, even members of the ICT team.

7.2 It is the responsibility of every staff member to lock screen if moving away from their device for any period of time even if for a minute to go to the photocopier. Locking your screen is quick and easy and can be done by pressing 'Ctrl, Alt and Delete' and selecting 'Lock' or by pressing the 'Window Key' and 'L' this will prevent people being able to access your network or email account.

7.3 When accessing your Council email on your personal device the provisions of this policy apply in the same way as accessing your email on a Council issued device. ICT have the ability to remotely remove access to your Council email if it is lost or no longer used for Council business.

8. Sending personal identifiable and confidential information

8.1 Under Data Protection Legislation, emailing personal or confidential data must be done securely and in line with minimum cyber security standards being met by both the sender and the recipient.

8.2 Sending emails from your surreyheath.gov.uk email to other government body, police or Social Services accounts is deemed secure if the organisation have met the secure email standards, a list of example email addresses and if they are likely to meet the secure standards is included below;

Recipient email address ends	*Secure*	*Additional actions required*
.gov.uk	*Yes*	*No*
.nhs.net	*Yes*	*No*
.cjsm.net	*Yes*	*No*
.police.uk	*Yes*	*No*

.mod.uk	*Yes*	*No*
.parliament.uk	*Yes*	*No*
Any other email address	*Not guaranteed to be secure.*	*Apply additional security (Egress) or send via password protected Box link*

8.3 If you are sending an email that includes personal identifiable and sensitive information and it is not going to the subject matter or one of the organisations that meets the cyber security standards then you must ensure that additional security measures are taken. Options include sending the information via a password protected BOX link or alternatively via Egress, (ICT can advise if this is not currently available to you). The encryption key/password must be sent separately to the main body of information and ideally communicated via alternative means for example a telephone call to the recipient. If you do not have access to a secure cloud sharing solution such as BOX please contact ICT who will be able to advise on the best way to share information.

8.4 You should only share personal and confidential information when there is a lawful basis and a need to know and this must be compliant with GDPR regulations (see: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/). Only minimum data may be shared and where possible the information should be anonymised or pseudonymised.

9. Data Loss Shield (DLS)

9.1 Data Loss Shield is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer or use of sensitive data via email. The Council has personal and sensitive information under its control that it must protect, to help us do this we have implemented the Data loss Shield (DLS) policy rules to all Council email users.

9.2 The purpose of the DLS policy is to protect the Councils personal and sensitive data by educating and raising awareness with staff when they are sharing data via email.

9.3 The DLS policy has been set up so that it will automatically pick up whereby users are sending personal and sensitive data outside of the Council to an insecure location. The DLS will activate an alert to the user which will require affirmative action before the email can be sent.

9.4 It is the responsibility of all Council email users to ensure where an alert has been received by the DLS that the email they are attempting to send is thoroughly checked ensuring that the personal and sensitive information within the email and complete email trail is appropriate to share with the recipients and in accordance with Council policy, seeking guidance from ICT/IG if unsure.

10. Unsolicited Email (spamming/phishing)

10.1 One of the biggest risks to the Council is cyber-attacks which may be received via phishing email. If you receive an email from an unknown source or receive an email you were not expecting that is asking you to click on attachments or links, stop and think, could it be a malicious. If you do receive an email that you think could be malicious close it down, do not forward it on or click on any attachments and contact the ICT Service Desk immediately.

10.2 To protect the email network, email messages are routinely scanned to ensure they do not contain viruses. Email messages that are suspected of containing viruses are blocked automatically. Email is also searched for offensive, abusive and/or racist language to protect email users from such material.

11. Managing your email box

11.1 Email messages can constitute all, or part, of a formal record of business. All members of staff are responsible for identifying and managing email messages that constitute a formal business record.

11.2 All departments should have in place processes or procedures which are understood by the whole department for identifying what is a formal business record and how emails should be managed as part of the formal record. When capturing emails as a formal record they should be saved as PDF rather than msg/eml and moved to a suitable storage facility usually a shared BOX folder or department system.

11.3 An email message that have been captured as a formal record and moved to the relevant location should be deleted from your mailbox. All other emails should be stored in accordance with the email retention policy.

11.4 If you have a requirement to save an email that is sensitive or cannot be shared with other members of your team you should move it to a suitable storage facility usually your personal BOX folder.

11.5 Any information or data created by you using your Surrey Heath email account belong to Surrey Heath Borough Council and not yourself.

12. Attachments

12.1 You should not send large attachments over email, especially to multiple email addresses, if the attachments are over 30MB they can be restricted and may not be received by the recipient, and increases the risk of information being shared excessively, instead a BOX link should be shared allowing the recipient direct access to the information. If the information contains personal or sensitive information the BOX link must be a secure link which is password protected and a time limit applied. If you do not have access to secure cloud sharing such as BOX please contact ICT who will be able to advise on the best way to share information.

13. Recipients

13.1 Always ensure that when emailing information you are sending it to the correct person at the correct email address. If you do mistakenly send an email to a wrong person and it includes personal identifiable and sensitive information, this is a breach of the Data Protection Act and must be reported in accordance with the SHBC Data Security Breaches Policy. If you do send an email to the wrong recipient, you must contact the recipient and ask them to delete the email immediately.

13.2 If forwarding or replying to an email check to make sure that no one else has been included in the email by checking the CC and BCC address boxes. You should also ensure only information intended for the recipient is included in the email, this will mean checking the complete email trail to make sure that you are not sharing excessive information. Excessive sharing of information is a Data Protection Breach and should be reported in accordance with the SHBC Data Security Breaches Policy.

13.3 The use of Blind Carbon Copy (BCC) emails may be a useful tool when sending out bulk email to a large number of staff or customers (for example an all staff email or a notification to more than one customer of a service cancellation) as it can remove email addresses that require protection from view. However great care should be taken when using them and the use of 'BCC' alone should not be relied upon to protect peoples personal data.

Sensitive personal data should never be included in a BCC email. If sensitive personal data needs to be sent to a group of people, then other more secure methods should be considered (for example bulk email services or secure data transfer services). BCC must not be used internally for small groups of people or to share information which may undermine an employee.

13.4 Although email is often considered to be a good way of disseminating information to large groups it should be noted that there are some restrictions. If a message needs to be conveyed to everyone in the Council you should consider putting it on Warbler instead e.g. leaver messages inviting staff to leaving parties. It should be noted that only

email messages that are considered to be of immediate interest to the majority of staff in the Council should be sent to everyone. All staff emails are restricted to Heads of Service, Service Managers and other designated officers. The list is held by the ICT Helpdesk.

14. Retention and Destruction

14.1 Emails are like any other record and must not be kept indefinitely. They must be managed throughout their lifecycle from creation to destruction. The email retention policy is 6 years on the main inbox and sent items folders and 4 years for Councillor emails. Emails must be managed in line with the relevant department retention and disposal policy and therefore if any email content is required for longer than 6 years under the retention and disposal schedules, it must be transferred to another storage medium such as BOX.

14.2 ICT reserves the right to place a retention policy on users mailboxes in line with this and other retention policies.

15. Accessing the mailbox of another member of staff

15.1 There may be occasions when it is necessary to access email messages from an individual's mailbox when a person is away from the office for an extended period, for example sick leave.

15.2 Examples of the reasons for accessing an individual's mailbox are: (this is not an exhaustive list)

- Subject Access Requests under the Data Protection Act.
- Freedom of Information requests.
- Evidence in legal proceedings.
- Line of business enquiry.
- Conducting an investigation which may result in disciplinary action.

15.3 Where it is not possible to ask the permission of the email user whose mailbox needs to be accessed, the procedure for gaining access to their mailbox is:

- Gain authorisation from the Head of Department
- Submit a request to the ICT Service Desk
- A record will be made for the reason for accessing the mailbox together with the names of the people involved.
- If appropriate inform the person whose mailbox was accessed.

16. Shared mailboxes

16.1 The creation of a shared mailbox should be done with a specific purpose, for example it might be created to discuss a particular policy area, to answer queries on a particular subject or there are a group of people responsible for the same area of work and can be a way of ensuring that queries are answered quickly.

16.2 The management of shared mailboxes is likely to be shared between everyone who has access to it. There will however be an 'owner' of the mailbox folder who will be responsible for the effective management of the folder and ensure the mailbox is used for its intended specific purpose. The owner will usually be the most senior officer with access to the mailbox.

16.3 Access to a shared mailbox is given by ICT. Authorisation must be in writing by the Line Manager or Head of Service via the ICT Service desk.

16.4 When managing shared mailboxes the lead person responsible for the mailbox should provide clear guidance and processes to all people who have access to the shared mailbox as to how the mailbox will be managed, these should include:

- the purpose of the mailbox

- who can access the mailbox
- how email will be managed/processed
- how long messages will remain in the mailbox before being removed (this should not be indefinitely)

17. Closing Accounts

17.1 When a staff member leaves the Council, they will work with their line manager to plan the handover of key pieces of work ensuring that important business emails are moved from their email to an agreed storage, usually within BOX or a relevant departmental system.

17.2 On leaving the Council, Council email users emails from the last 6 months will be retained for a further 6 months, unless a CMT member requests that the emails be kept for longer due to business requirements. After 6 months the email account will be deleted.

17.3 After the email user has left the Council and during the 6 month period the email is still retained, key emails can be requested from the IT service desk with HR Manager/Head of Service agreement for example if there is an investigation or a business-critical requirement such as finding a key decision for audit purposes. The search criteria must be in accordance with the business need.

18. Personal Email

18.1 Your personal email account must not be used for Council business. Your official SHBC email account is the only approved email system.

18.2 Whilst it is appreciated that there will be occasional personal emails sent from or to a Surrey Health email address, this must not be excessive. If unsure, please seek the advice of your line manager.

18.3 When emailing SHBC staff and Councillors on Council business you should always send to their Council email address and not their personal address. If a staff member or Councillor emails you from their personal

address and it is Council business, you should respond to their Council email, politely emailing their personal address asking them to check their Council email.

18.4 You must not automatically redirect emails from your Council email to a personal email address.

19. Misuse/abuse of email

19.1 Misuse of Council email may make both the email user and the Council liable under law (please see section 22) and may impede the function of the Councils IT systems and email. All Council email users are responsible for ensuring that email is used appropriately and in compliance with this policy.

19.2 Only authorised personnel can access Council email accounts. Do not log other people onto any Council email account.

19.3 You must not subscribe to non-work related mailing lists, social medias, and networking using your Council email address.

19.4 You must not use your Council email for personal commercial gain. This includes but is not limited to unsolicited marketing, advertising and selling of goods or services.

19.5 The forwarding of spamming emails, jokes or materials designed to/or likely to cause annoyance or offence is not permitted.

19.6 Deliberate misuse of Council email will be investigated in accordance with the Councils disciplinary policy.

20. Monitoring of Email

20.1 The Council uses an email scanning service that scans incoming and outgoing email traffic for all Council email users. This system is designed

to filter out malware that is attached to electronic mail messages and phishing attempts. It is important to note that this system captures a large number of malware but there is still the potential for malware or phishing emails to slip past this system, so vigilance when opening emails is still essential.

20.2 To try and prevent the loss of personal confidential data over email, the Data Loss Shield (DLS) tool within outlook scans email for personal or confidential data that is being sent to an insecure external email address. If it is identified by the DLS that an email has been sent inappropriately it will be raised with the IG or ICT Department to review as a potential Data Protection breach.

20.3 To try and combat the risk of cyber-attack, the council undertakes regular staff training campaigns in a real time work environment via email, results from these training campaigns provide the ICT team with overall statistics as well as identify any high risk staff, enabling us to close the security gap.

20.4 The content of email messages is not otherwise routinely monitored. However, Council email users are advised that the content of email messages can be and will be monitored if they are suspected of misusing the email system. Before the monitoring can take place the ICT Helpdesk require approval from, a line manager or Head of Service. If no further action is to be taken as a result of monitoring the content of email messages then all the data collected as a result of the monitoring will be destroyed immediately. If further action is taken as a result of monitoring the content of email messages the data will be stored for disciplinary purposes.

21. Incident reporting

21.1 It is the responsibility of all Council email users to report breaches of this policy to their line manager and/or IG Manager. The Council need to mitigate any breaches and learn from mistakes. The actions required following a potential breach will depend on the level of sensitivity and amount of information disclosed. The Data Security Breaches Policy gives more information on the data breach process.

21.2 Incidents of inappropriate activity identified via the DLS are monitored by the IG Department, any egregious activity or repeated breaches of this policy identified by the DLS will be reported to the Line Manager, and where appropriate HR.

21.3 Any malicious or repeated inappropriate use of email will be investigated by the ICT Manager and/or IG Manager, relevant Line Manager and HR, in accordance with the Information Security Breaches Policy and Disciplinary Policy.

22. Related Law

This section sets out key legislation and common law affecting the use of email.

The General Data Protection Regulation (EU) and Data Protection Act 2018 Sets out the conditions for the processing of personal information by organisations and individuals. Staff need to be aware that any use of personal information stemming from work related business can only be used where conditions of the Act can be met. Organisations are legally required to ensure the security of personal information that they process.

Subject Access Requests Individuals have the legal right to request personal information that is held on them by organisations processing personal information such as Local Authorities. Requests could come from individuals such as service users, complainants, and Council staff - this is known as a Subject Access Request. It could be possible that following receipt of a subject access request, that email content that an Council email user holds and/or has produced could be subject to release as part of a request where those emails contain personal information relating to the individual. Where such a request is received, staff may have to search through their emails and filing systems for any relevant email content for consideration of release.

Freedom of Information Act 2000 Allows the right of access to anyone to recorded information held by a public authority through either a request for specific information or through accessing information via the Publication Scheme. Release of information is subject to exemptions and conditions of the Act. Information held on a Council email users communications may be caught by the Act if they are relevant to a specific request that has been received. In which case, the Council email user would need to search for relevant email content and provide that content to the Freedom of Information processing team

Human Rights Act 1998 Article 8 of the Act provides a right of privacy for individuals. In complying with the Act, public authorities (to which the Act applies) such as the Council need to ensure that personal and confidential information is not disclosed unless a legal justification exists to do so.

Privacy and Electronic Communications Regulations 2003 The Regulations cover marketing by electronic means, including marketing calls, texts, emails and faxes. The Regulation specify a clear need for

consent when emailing or texting individuals for marketing. It should be noted that the definition of 'marketing' is very broad and including seeking to influence individuals behaviour.

Computer Misuse Act 1990 Under this Act it is an offence to have unauthorised access to computer material or to undertake unauthorised modification of programs or data on a computer.

Payment Card Industry Data Security Standards (PCI) This sets the information security standards for handling credit/debit card data to reduce credit card fraud and protect cardholders data from unauthorised access. The standards govern the way card numbers are transmitted, processed and stored, emailing full numbers is against the standards as it is not a secure transfer of data.

Document revisions

Document revised (date)	Details of revisions made	Version
February 2024	Initial revision	1