The Linden Centre

Email Policy

Signed by:		
	Headteacher	Date:
	Chair of Management Committee	Date

Last Updated	12/12/2022
Review Due:	12/12/2024

S2 Use of Email/Teams/Other Communication/Video Conferencing Technologies (v6.0)

Email/Microsoft Teams and other communication technologies are a valuable business tool. However staff must be aware that emails, saved Teams conversations and other electronic messages have the same legal status as other documents and in particular email attachments may be shared very quickly to readers across the world. Remember that contents of emails and/or any saved conversations using Teams or other communication technologies can be disclosed when requested under the Freedom of Information Act 2000.

Good management of staff mailboxes is essential for proper records management. It is also important as size of files and storage can easily get out of control, costing the Council time and money. The Council reserves the right to impose mailbox quotas on any or all staff in the event that storage becomes an issue.

IMPORTANT - Private Usage

Limited personal use of the Council's email system, Teams and other communication technologies is acceptable but this use must be confined to outside an officers working hours and staff must still abide by Council rules on acceptable and unacceptable use set out below.

The following conditions must be followed:

Acceptable – Staff must

Use the Council's Secure Communication System (SCS) to exchange personal and sensitive data to external parties where TLS enabled email cannot be used

Ensure that a generic/team email account is only used in appropriate circumstances such as information which is relevant to each team member and not using the account to send confidential information which should only be shared with certain team members

Ensure they send an email to the correct person, always double check the recipient. They must also limit the number of recipients of the email to people who require it to do their job or are bona fide recipients

Limit the amount of personal data in the body of the email or in attachments to only that which is needed

Where possible provide a link to documents in an email to reduce the number of copies held of a document

Remind the recipient, if any sensitive/confidential data, of their responsibility for the security and confidentiality of that data.

When confidential/sensitive data is received by email it should be deleted from the email system as soon as possible and filed/secured appropriately, either electronically or on paper.

When confidential/sensitive data is received by email it should be deleted from the email system as soon as possible and filed/secured appropriately, either electronically or on paper.

When “forwarding” emails or using the “reply all” facility consider whether the content is suitable for everyone on the list of recipients, as confidential/sensitive data could be sent in error

Only use “bcc” (blind copy) in an email on an exception basis, after careful consideration - the message may be forwarded by the recipient as “reply all” to the “bcc”. This would mean that all details will be revealed to the other people on that email list

Use a dedicated room when using Teams video

Adhere to corporate standards for email signatures

Unacceptable – Staff must not

Use their Council email address for personal use, e.g. register it on a non-work website

Respond to suspicious (spam) emails, if they have any doubts about who has sent the email then the email should not be opened or replied to

Click on any untrusted web links detailed in a suspicious email or open any attachment as they may contain viruses.

Use email/Teams/other communication tools to send personal messages in work time and/or that are inappropriate, abusive and malicious

Access an email/Teams/other communication tool for which they are not authorised

Use email/Teams/other communication tools for any private gain including running a business or associated advertising

Keep received, sent or deleted sensitive/confidential data on the email/Teams/other communication tools longer than necessary

Send or forward confidential information outside the Council without appropriate security in place including strong passwords and encryption, e.g. use of SCS or TLS enabled mail

Forward Council emails to their own personal email address

Use the Councils email/ Teams/other communication tools in any way that could damage the reputation of the Council and/or its staff

Represent their own opinions as those of the authority

Send emails that infer that they are an official document when that is clearly not the case.

Click on any links or follow any instruction in an email received from an unknown source. Emails of this nature can contain malicious content, if officers are unsure as to whether they should open an email or follow any subsequent instruction they should contact ICT

Automatic Forward Rules (email)

The use of automatic forwarding rules where work emails are automatically forwarded to another non work (not @telford.gov.uk or @taw.org.uk) is disabled. This is due to work emails potentially including personal/confidential data that could be forwarded to another non work email account will little/no protection in place.

Use of SMS (text)

Staff should be aware that any communications with colleagues and/or customers are business records and therefore they should be managed accordingly. Staff are increasingly using SMS as a way of communicating with customers in particular, as this is the customers preferred method of communication.

However please note SMS is **NOT** a secure means of communication and therefore should:

- Only be used where there are no other viable alternatives
- Not be used to communicate personally identifiable information
- Only be used on a mobile phone provided by the Council

A record should be held on a business record that the SMS communication has taken place.

Use of Video Conferencing Technology (VCT)

Council staff are increasingly using video conferencing technologies to meet and/or collaborate with third parties. The Council preferred choice of VCT is Microsoft Teams and must always be used wherever possible.

Where the use of Microsoft Teams is not viable, ICT should be consulted about the potential use of alternative solutions.

When using Microsoft Teams, the requirements of the CISP should be complied with.

Security & Monitoring

Security	Monitoring
• Private, confidential, personal or sensitive information should not be revealed or sent by email except to Telford & Wrekin staff and/or school staff also on the same email system, i.e. all staff with a @telford.gov.uk or @taw.org.uk. When unsure whether content is suitable for sending by external email ask yourself "*if this information was about me, my family or my company would I want the information available for anyone to see?*" • Secure email systems such as TLS enabled	• If any emails are stopped by the content filter they may be read by an appropriate ICT officer, if the decision to stop the email is challenged. • The Council reserves the right to access, read and monitor emails/Teams messages or other electronic communications that are transmitted over Council networks or stored on Council equipment. • Monitoring of activity will take place, in line with Lawful Business Practice Regulations

mail and the Council's Secure Communication System (SCS) exist for the secure transfer of personal / sensitive information to external bodies and therefore should be used.
- Before sending emails staff must consider whether it is essential to include full names in external emails where abbreviations or reference numbers could be used, so that individuals cannot be identified.
- An email should be treated in the same way as a paper record regarding retention or deletion. Further information on retention/deletion of records can be provided by Information Governance

2000 and only when it is appropriate to do so.
- Misuse of email/Teams/other electronic communication technologies could result in temporary or permanent withdrawal of access and may be dealt with under the disciplinary process of the Council. Separate legal proceedings may be necessary including seeking prosecution under the Computer Misuse Act 1990.
- Email/saved Teams or other electronic messages may need to be accessed by management when staff are absent from work, and signing this policy will constitute acceptance of this.

Staff should also note:

- **Out of office** - 'Out of Office' assistant should always be used for planned absence. All out of office messages should comply with Corporate Communications requirements and must contain as a minimum the statement *"If this is a request under the Freedom of Information Act or similar legislation, please send your request to foi@telford.gov.uk*". Where absence is unplanned officers should activate their out of office message via a works mobile device or by Web Mail. If this is unachievable managers will ask ICT to activate the 'Out of Office' message.

- **Outlook calendar** - With the move to Office 365 officers should not save personally identifiable data in the subject of their outlook calendars. Any exceptions to this must be approved by the relevant Assistant Director (Information Asset Owner).

Key Messages to Staff

- **All emails sent and received using the Council's system will be automatically scanned and filtered**
- **Officers emails/Teams messages and other electronic communications will be monitored if it is deemed appropriate to do so. This will include any private emails**
- **Misuse of email/Teams/other communication technologies can lead to disciplinary or criminal proceedings**
- **All emails/Teams and other messages communicated electronically on Council systems remain the property of the Council and may need to be disclosed under the Freedom of Information Act 2000**