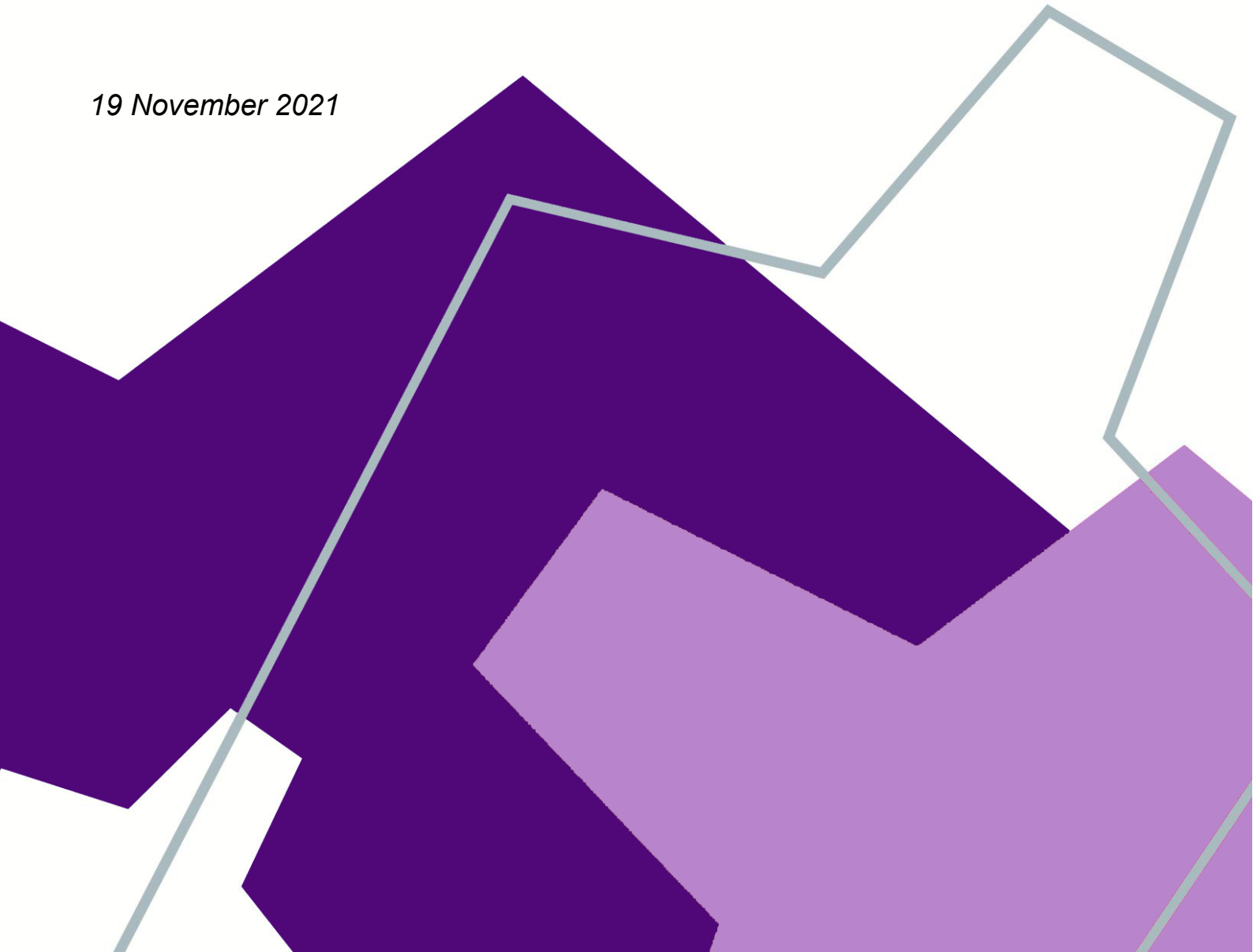
The Scottish Parliament
Pàrlamaid na h-Alba

Acceptable use of IT policy

Poileasaidh air Cleachdadh IT Iomchaidh

19 November 2021



Introduction

This policy sets out the SPCB's position on the use of its IT systems. It also covers your use of social media through channels internal to the Parliament and in your personal life.

You are trusted to use social media and the SPCB's IT systems in a sensible and responsible manner, exercising good judgement. This policy is intended to support you in doing so by setting out what is and is not considered acceptable, both from an organisational and legal perspective.

The SPCB's IT systems which are covered in this policy include, but are not limited to:

- Email and Internet;
- The Document and Records Management System (SPShare); and
- Telephones.

All forms of social media are covered in this policy including, but not limited to:

- internal platforms such as SPShare and Sharepoint;
- external platforms such as Facebook, Twitter and LinkedIn; and
- all other internet postings, including blogs and group forums.

Staff in particular roles are authorised to use our official social media channels to engage with the public about the Parliament and this use is covered by the Corporate Social Media Policy. Further guidance is available from the Parliamentary Communications Office.

Scope

This policy applies to all SPCB staff, staff on secondment and contractors who are authorised to use the SPCB's IT Systems.

Breaches of Policy

In the rare event that there is an alleged breach of this policy, this will be dealt with in accordance with the SPCB's Disciplinary Procedures. Sanctions up to, and including, dismissal may be imposed. If you are a member of contractor's staff and you are found to be in breach of this policy, this will be reported to the contract manager and your services may be terminated under the terms of the contract. If it is suspected that the SPCB's IT systems are being used for anything illegal, these concerns will be reported to the police or any other relevant authority.

Monitoring and Review

This policy is subject to regular monitoring and review to take account of legislative changes, identified best practice and experience.

Principles

The principles under which you are authorised to use the SPCB IT systems are as follows:

- The SPCB requires that all use of its IT systems by you is primarily for business purposes. You may, however, use the systems for limited non-business use if you do so in your own time, for example, on your lunch break or before or after work. You may also use these systems to deal with brief, important, personal matters so long as this does not interfere with the completion of work.

- The SPCB's IT systems automatically record information on activity and access, and use can be attributed accurately to individual users. In line with relevant legislation and IT security best practices, the SPCB reserves the right to review these records to ensure adherence to this policy. This means that you must not expect to have total privacy, for example, in any messages you send or receive or in your use of the internet

- You must observe the terms of the SPCB's Equality Framework and Dignity at Work policy in using its IT systems and in your use of social media.

Queries

Should you have any queries in relation to use of the SPCB's IT Systems, please contact the IT Helpdesk on Extension 86100.

System and Information Security

Information Security

You are responsible for any action carried out under your IT account and must take all reasonable steps to ensure that you do not unnecessarily compromise the security of the Scottish Parliament's information and associated assets. Further guidance can be accessed through BIT's Information Security Guide. To avoid misuse, you should:

- lock your workstation when away from your desk

- ensure that you log out of your account when you are finished

- never divulge your password to anyone

- never attempt to log on to, or use a network account that is not yours.

Viruses

Viruses can be introduced through use of email and the internet. You must take all reasonable steps to ensure that you do not knowingly allow a virus to affect the SPCB's IT systems and that no viruses are transmitted by you to any third parties. The deliberate introduction of a virus onto a third party's IT systems may be a criminal offence whilst accidental introduction may, in certain circumstances, give rise to a claim against the SPCB by that third party. All e-mail transmitted via the SPCB network is automatically scanned for viruses. Since a virus may, nevertheless, slip through, please beware of all unsolicited e-mails and e-mails from unknown sources. You may also receive e-mails warning of viruses, encouraging you to forward the e-mail on to others. These are usually hoax messages designed to overload IT systems.

If you have any reason to be suspicious, do not open or run any attached file or forward any message. Please contact the IT Helpdesk immediately on 86100.

Acceptable Use of IT Systems

Unless strictly necessary for the proper conduct of your duties, the SPCB's IT Systems must not be used for the creation, transmission, downloading, browsing, viewing, reproduction or accessing of any image, material or other data of any kind which is illegal or otherwise unacceptable to the SPCB. This includes, but is not limited to:

- material of a sexually explicit nature including messages, images, cartoons or jokes (including nude or partially dressed men or women)

- anything which may harass, bully or discriminate against any individual or group of people. This includes malicious gossip and messages that contain an aggressive or abusive tone, style and/or content

- posting or otherwise sharing data which breaches the confidentiality of information relating to the organisation, Members, contractors or colleagues

- material which is, or is potentially, defamatory and/or material which is likely to cause embarrassment to the Parliament.

You are not permitted to use the Parliament's logo or corporate branding on personal web pages or social media channels

- material which is likely to introduce viruses or other unauthorised software into the SPCB's IT systems

- material which is concerned with your own commercial enterprise or conflicts with the interests of the SPCB

- material which unnecessarily disrupts the work of colleagues.

If you have any doubt as to whether a particular activity is/is not permissible, you should ask the IT Helpdesk before acting. You should also note that the prohibitions in this policy still apply even if the material is located on a part of the systems which is personal or password protected.

These restrictions apply to both business (unless otherwise stated) and personal use. The SPCB considers that it is important that all use is restricted in this way to avoid disruption in the workplace and embarrassment, distress or offence to others.

Use of Email and Internet

Use of Email

In using email, you should bear in mind that it is not a secure means of transmitting information due to the risks that it may be intercepted, copied and widely distributed and/or inadvertently sent to the wrong person/organisation. It is important that you do not delete, alter or otherwise interfere with the disclaimer which is automatically attached to emails sent from the SPCB systems.

Commercial and Legal Effects of Email

The commercial and legal effects of sending and receiving emails are the same as any other form of written communication. The style, tone and content of emails have a direct effect on the way the SPCB, and indeed the Parliament itself, is perceived by others. Emails can contractually bind the SPCB and any commercial advice, opinion, guarantee, representation or other statement contained in an email may be relied upon by third parties. You must not, therefore, send emails which make representations, contractual commitments or any form of legally binding statement concerning the SPCB unless you have specific authority to do so. It is your responsibility to ensure that appropriate

records are retained in accordance with the SPCB records retention schedule, including records of any commercial or legally binding emails which are sent in the course of SPCB business. Such emails should be captured in the document and records management system.

Records

As contents of the email system are archived regularly, you should file all essential emails in the Document and Records Management system in the appropriate area to create a record for ease of retrieval. You should regularly delete messages which do not require to be retained.

Specific Circumstances

In circumstances where you:

- receive an unacceptable email from someone, you should not reply to the email. If the sender is someone you know, you should ask them not to send such material in future. If the email is from within the Parliament, you should report the matter to your line manager who may raise it with the HR Office. If you do not know the sender, you must not reply to the email, rather you should contact the IT Helpdesk (86100), for advice

- receive a chain letter, junk mail or unsolicited commercial or advertising materials, you should delete them immediately, without replying or forwarding these on. Do not click on any "unsubscribe" link as this may simply confirm to the sender that your email account is active

- enter an internet site carrying offensive material by accident, you should immediately close your browser and report the matter to the IT Helpdesk (86100). Such access will not be considered a breach of this policy if you do this and the incident will be registered to ensure no further action is taken.

Unacceptable Use

You are not permitted to:

- create, transmit or download chain letters, junk mail or unsolicited commercial or advertising email

- download any software, audio files, games etc. from the internet or to install or use any unauthorised software or hardware from home to use on the IT systems unless such activity it has been approved by BIT. If you require any particular business related software, please submit an IT Work Request

- access or attempt to access anyone else's email account without their permission. In emergency cases the appropriate line manager may request a password reset on a member of their staff's IT account and he/she will be notified of the temporary password to allow him or her to access the account

- use email or the internet to impersonate others or to forge messages or email addresses. Where a message is sent on behalf of another person the message should make it clear that this is the case and should identify the writer and the sender

- browse, access or use any internet site in any manner which breaches its published terms and conditions or download or store any material without reading and complying with any copyright or license restrictions. In addition, you must not store any copyright material (eg audio or video files, installation files, etc) on the SPCB's IT systems if it is not directly related to the business of the Parliament.

Use of the Document and Records Management System

Access to Information

The Document and Records Management system is an open-by-default system which enables staff to operate in a collaborative environment. You should only access information stored in the Document and Records Management system where you have a genuine business reason for doing so. Similarly, you must not provide access to anyone unable to access information contained within the system. It is important to note that the system maintains an audit log of activity concerning documents and records held within it.

Safeguarding Information

The Parliament's Protective Marking system should be adhered to in order that information is safeguarded in terms of its storage, security, distribution and destruction. Specifically, you should use the Document and Records Management system's protective marking feature whenever it is necessary to send sensitive information internally. Documents and records should not be distributed internally as email attachments but should be shared as links from SPShare. This ensures that information remains secure and maintains a complete and accurate audit trail of activity.

Use of Private Storage Areas of the DRM (MySites)

Within the DRM system are private storage areas (currently known as MySites) that give you a central location to manage and store private, work related content which colleagues do not require access to (e.g. performance appraisal documents). You should bear in mind that whilst designated as private sites, these areas are nonetheless corporate resources. As such you should not expect to have total privacy for the content stored on Parliament systems and you should be aware that all information stored on corporate systems may be subject to Freedom of Information requests.
The following items may not be stored in your personal areas of the DRM system:

- Photographs
- Music and video files; and
- Copyright restricted files

As only you will normally have access to your own private area of the DRM system, corporate information should not be stored here. The information and records produced or received by the Scottish Parliament during the course of its business activities are owned by the SPCB and not by the individuals who compile or receive them. It is important to ensure that corporate information is saved to an area where it can be accessed and used as a corporate resource.

Use of Social Media

All forms of social media are covered by this policy, including internal platforms provided for professional use and external channels used in both a professional and personal capacity. In terms of use of social media in your personal life, this policy applies whether use is in the workplace or outside it, during working hours or otherwise and regardless of whether the social media is accessed using any of the SPCB's IT systems or any personal equipment.

Use of the Parliament's official social media channels is covered separately through the Corporate Social Media policy. There should be a clear distinction between anything you post in a business capacity through the Parliament's official social media channels and anything you post in a personal capacity through your own social media profiles. The relevant approval mechanisms should be followed via the Web and Social Media Team before posting from an official Parliament profile. You should feel free to like or follow official Parliament pages from your personal accounts.

The SPCB positively encourages the use of social media to connect, communicate and collaborate in ways which add value to the Parliament. As such, it does not intend, through this policy, to prevent you from conducting legitimate personal and business activities via social media. Rather, guidance is provided to empower you to take advantage of the opportunities which social media offers whilst avoiding the pitfalls that can result.

You can exploit the advantages of social media for a variety of means, including:

- Engaging others in your work and keeping them informed
- Generating ideas and feedback
- Promoting initiatives/projects and explaining concepts
- Following discussions and keeping track of news
- Sharing good practice and making recommendations
- Building and extending networks

You have a personal responsibility for everything you post, whether through internal or external social media channels. You should be aware that social media postings are instantly available to other users, nearly impossible to erase and will be considered "public" regardless of whether or not the account settings ensure private or restricted access.

In light of the above, you must ensure that in your use of all social media, you observe the SPCB's policies, including the Code of Conduct, and avoid taking any action that would bring the Parliament into disrepute. This includes, but is not limited to, ensuring that any posts you make are in line with the Parliament's values, that you are politically impartial and that you protect confidential information. Confidential information includes information obtained through working at the Parliament which is not in the public domain and the use of personal data of colleagues without their permission. You must also treat others with respect by not making any comments which are offensive, disparaging, derogatory, discriminating or defamatory. You are trusted to exercise common sense and good judgment and to seek early advice from your line manager if you are in any doubt as to what is acceptable.

Specific to your use of social media in your personal life, you may identify yourself as a Parliamentary employee. What you do in your personal life is, generally speaking, your own business. You should be aware, however, that as an employee you represent the Scottish Parliament to the world – whether acting on the Parliament's behalf of your own. It is important to be mindful that personal views or information expressed on social media cannot be entirely isolated from your working life. Your actions and behaviour on social medial therefore have the potential to positively enhance or adversely impact the Parliament's reputation and appropriate care should be exercised to comply with the Code of Conduct at all times.

Any breaches of this policy or other relevant SPCB policies (including the Code of Conduct) may result in disciplinary action being taken up to, and including, dismissal.

Use of Telephone and Other Business Communications Systems

The SPCB recognises the occasional need to make short, important, personal telephone calls using its network. In the case of SPS staff this is allowed so long as this does not interfere with the completion of work or disturb colleagues. No one, however, may make personal use of international calls, unless:

- they are working abroad and have come to an arrangement with their line manager; or

- they make arrangements to reimburse the cost of the calls.

If you have been supplied with a mobile phone, you may only use it for personal calls:

- if you have reached an agreement with your line manager as to what are reasonable personal calls; or

- if you inform your cost centre manager and make arrangements to reimburse the cost of these calls, if they amount to more than £5.

You may also use the fax system for personal use, provided you make arrangements to reimburse the cost.

You may not, however, under any circumstances, use the SPCB's postage or stationery for personal purposes.

Privacy and Monitoring

It is not the SPCB's intention to routinely monitor data which is transmitted over its IT systems. This data is, however, automatically logged and includes the viewing, creation and editing of documents and records. We may, from time to time, monitor the systems for the following purposes:

- to ensure the SPCB's practices, policies and procedures are being followed

- to investigate or detect the suspected unauthorised use of the SPCB's IT systems

- to secure the effective operation of the SPCB's IT systems

- to maintain a complete and accurate representation of all changes that occur in relation to particular records in order to comply with the requirements of the Public Records (Scotland) Act 2011

- for the purpose of preventing or detecting crime

No audit information is captured from personal MySites. If you are absent from work, or in the event of an emergency it may be necessary to:

- check your email inbox to ensure that mail items are dealt with appropriately in your absence. This will only be done if authorised by your line manager in writing to the IT Helpdesk. E-mails which are clearly personal or private will not be checked unless we have your prior permission

- check-in any documents you have checked-out in the document and records management system. This policy will be operated in line with the SPCB's Data Protection Policy in Relation to Employee Information.

Acceptable use of IT policy

For further information contact:

HumanResources@parliament.scot

0131 348 6500