Acceptable use policy, personal use, and employee privacy: Ten questions answered

October 01, 2025

User behaviour is central to maintaining strong organizational data security. The “Acceptable Use Policy” (AUP) has long been a key tool for guiding user behaviour, protecting networks, and asserting strong control over organizational data. Courts and labour arbitrators now recognize a limited employee right to privacy when using organizational networks for personal purposes. While this right does not compromise network security, it must be carefully addressed in AUPs.

Below are answers to ten common questions organizations ask about maintaining effective AUPs while respecting employee privacy.

1. What should organizations do to ensure their AUPs address personal use?

Organizations should ensure their AUPs (1) clearly state all reasons management may access and use information stored on the system, and (2) emphasize that personal use is a voluntary choice that involves giving up some privacy. This recent arbitration decision highlights the benefits of highlighting this choice.

2. What are the most common purposes for organizational access?

Consider the following list:

a. to engage in technical maintenance, repair, and management;
b. to meet a legal requirement to produce records, including by engaging in e-discovery;
c. to ensure continuity of work processes (for instance, employee departs, employee gets sick, work stoppage occurs);
d. to improve business processes and manage productivity; and
e. to prevent misconduct and ensure compliance with the law.

3. How should organizations define the scope of an AUP?

AUPs typically apply to “users” (employees and others) and the “system” or “network.” To manage privacy expectations, policies should clarify that company-owned devices (laptops, handhelds, etc.) issued for work are part of the system.

4. How should access control be framed in an AUP?

Access controls based on the “least privilege” principle are vital for information security. These controls benefit the company and should be framed as such, not as privacy protections for employees.

5. How should passwords be addressed in an AUP?

Password sharing should be prohibited. Employees must keep passwords secure.

Passwords are for organizational data security, but – remarkably – have been confused by courts as supportive of employee privacy; see this famous case. AUPs should clarify that passwords help organizations identify users and do not prevent organizational access.

6. Does access to forensic information raise special issues?

Yes. AUPs should inform employees that system use may generate hidden data (such as log files or deleted information) that the employer may access during investigations or otherwise.

7. How should an organization address the use of personal devices?

While using only company-owned devices is safest, many organizations adopt “Bring Your Own Device” (BYOD) policies. Employers should use technical and legal measures to secure the network and control corporate data on personal devices. For example, requiring remote management of personal devices as a condition of use, with an understanding of reduced privacy.

8. Should an acceptable use policy govern the use of social media?

Only indirectly. AUPs govern corporate network use, while social media policies address Internet publications from any device. Employers should clarify that home-based publications are not necessarily private, and avoid mixing social media rules into AUPs.

9. Should organizations utilize annual acknowledgements?

Generally, annual acknowledgements are not required to enforce AUPs. The key is providing clear notice of terms. A login script with warning language is helpful. For example: “Use a personal device unconnected to our system for confidential personal communications and file storage.”

10. Are there special concerns for public sector organizations?

Public-sector employers in Canada can be subject to the *Canadian Charter of Rights and Freedoms* and freedom of information laws. Many have unionized workforces. While guidance is similar to private organizations, public-sector employers must carefully manage employee expectations due to their legal context.

Contact us

BLG’s Cybersecurity, Privacy & Data Protection Group closely monitors rapidly evolving cyber security and privacy legislation, and can assist you in planning your organization’s strategy around matters of acceptable use policy, personal use, and employee privacy. Please reach out to the key contacts below with any questions you may have.

By

Daniel J. Michaluk

Expertise

Cybersecurity, Privacy & Data Protection, Information Technology, Labour & Employment

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749