Literasi Digital

Teori, Praktik, dan Tantangan

Daniel Pandapotan, Latifah, Phie Chyan, Arif Muhamad Nurdin, Rizky Ridwan, Effendi, Agung Yuliyanto Nugroho, Alya Felisha, Litha Mutriwana, Rossanita Truelovin H. P, Seri Wahyuni, Christina Maya Iriana Sari, Muh Fajar Fazriansyah, Muhammad Natsir Maulana, Fransiskus Mario Hartono Tjiptabudi, Bayu Kusumo, A.Kachsyfur Djasim Ilyas Paenrongi, Setia Rahayu Niate, Ari Widiastono, Novaldo Dewangga Priantara

Literasi Digital

Teori, Praktik, dan Tantangan

Daniel Pandapotan, Latifah, Phie Chyan, Arif Muhamad Nurdin, Rizky Ridwan, Effendi, Agung Yuliyanto Nugroho, Alya Felisha, Litha Mutriwana, Rossanita Truelovin H. P, Seri Wahyuni, Christina Maya Iriana Sari, Muh Fajar Fazriansyah, Muhammad Natsir Maulana, Fransiskus Mario Hartono Tjiptabudi, Bayu Kusumo, A.Kachsyfur Djasim Ilyas Paenrongi, Setia Rahayu Niate, Ari Widiastono, Novaldo Dewangga Priantara

PT. MIFANDI MANDIRI DIGITAL

Undang-Undang No. 28 Tahun 2014 Tentang Hak Cipta:

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam pasal 9 ayat (1) huruf i untuk penggunaan secara komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp. 100.000.000,- (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk penggunaan secara komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp. 500.000.000,- (lima ratus juta rupiah).
3. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk penggunaan secara komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau pidana denda paling banyak Rp. 1.000.000.000,- (satu miliar rupiah).
4. Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp. 4.000.000.000,- (empat miliar rupiah).

Literasi Digital
Teori, Praktik, dan Tantangan

Daniel Pandapotan, Latifah, Phie Chyan, Arif Muhamad Nurdin, Rizky Ridwan, Effendi, Agung Yuliyanto Nugroho, Alya Felisha, Litha Mutriwana, Rossanita Truelovin H. P, Seri Wahyuni, Christina Maya Iriana Sari, Muh Fajar Fazriansyah, Muhammad Natsir Maulana, Fransiskus Mario Hartono Tjiptabudi, Bayu Kusumo, A.Kachsyfur Djasim Ilyas Paenrongi, Setia Rahayu Niate, Ari Widiastono, Novaldo Dewangga Priantara

ISBN: 978-634-7226-24-2

Editor : Sarwandi, M.Pd.T
Layout : Miftahul Jannah, M.Kom
Desain sampul : Rifki Ramadan

Penerbit
PT. Mifandi Mandiri Digital

Redaksi & Distributor Tunggal
PT. Mifandi Mandiri Digital
Komplek Senda Residence Jl. Payanibung Ujung D Dalu Sepuluh-B Tanjung Morawa Kab. Deli Serdang Sumatera Utara

Cetakan Pertama, Juli 2025

Kata Pengantar

Perkembangan teknologi informasi dan komunikasi yang begitu pesat telah mengubah secara fundamental cara manusia belajar, bekerja, berinteraksi, dan bahkan berpikir. Di tengah derasnya arus digitalisasi, kemampuan untuk memahami, memilah, dan menggunakan teknologi secara bijak menjadi sangat penting. Dalam konteks inilah, literasi digital hadir bukan sekadar sebagai keterampilan teknis, tetapi sebagai fondasi kecakapan hidup abad ke-21 yang melibatkan aspek kognitif, sosial, etis, dan kritis dalam penggunaan teknologi digital.

Buku Literasi Digital: Teori, Praktik, dan Tantangan ini disusun sebagai panduan komprehensif untuk memahami berbagai dimensi literasi digital secara utuh. Dimulai dari konsep dasar dan framework literasi digital, buku ini menjelajahi isu-isu krusial seperti keamanan siber, hak dan kewajiban digital, fenomena berita palsu, cyberbullying, hingga tantangan etika dan privasi. Tidak hanya membahas teori, buku ini juga memaparkan praktik terbaik, strategi pembelajaran, studi kasus nyata, serta integrasi literasi digital dalam dunia pendidikan melalui pemanfaatan AI, IoT, e-learning, hingga Metaverse.

Kami berharap buku ini dapat menjadi rujukan penting bagi pendidik, pelajar, pembuat kebijakan, dan masyarakat umum dalam membangun kesadaran digital yang bertanggung jawab dan reflektif. Lebih dari sekadar mampu menggunakan

teknologi, pembaca diajak untuk memahami dampaknya, bersikap kritis terhadap informasi, dan berpartisipasi aktif dalam ruang digital secara etis. Semoga kehadiran buku ini dapat memperkuat peran literasi digital dalam menciptakan masyarakat yang inklusif, adaptif, dan berdaya saing di era transformasi digital yang terus berkembang.

Medan, Mei 2025

Penulis

Daftar Isi

BAB 1 LITERASI DIGITAL

Pendahuluan

Di era ledakan informasi, kita tidak lagi kesulitan untuk menelusuri, mencari, dan memperoleh informasi. Berbagai teknologi dan jenis media telah tersedia dan mudah diakses. Mulai dari mesin pencari (*search engine*), *platform* media sosial, hingga kecerdasan buatan berbasis *natural language processing* (NLP) seperti ChatGPT, Gemini, dan sebagainya. Selain itu, akses ke database artikel ilmiah nasional dan internasional, prosiding, dan repositori digital semakin mempermudah kita dalam menelusur sumber informasi yang kredibel dan relevan.

Yang dibutuhkan adalah kemampuan memfilter informasi dan mendapatkanya secara cepat, tepat dan akurat. Hal ini mendorong pemahaman bahwa seseorang yang mampu mengoperasikan berbagai tools secara online sebagai seseorang yang literat digital dan ini seringkali diterjemahkan sebagai literasi digital. Seolah-olah literasi digital hanya berarti mampu mengoperasikan perangkat teknologi seperti membuka HP, menginstal aplikasi, browsing dan mengirim email.

Pemahaman seperti ini keliru dan tidak memadai karena hanya menyentuh aspek keterampilan teknis paling dasar yang lebih tepat disebut sebagai digital skills, bukan digital literacy. Literasi digital sejati jauh melampaui sekadar penggunaan perangkat; ia mencakup kemampuan berpikir kritis, etis, dan bertanggung jawab dalam memanfaatkan teknologi digital

untuk pembelajaran, pekerjaan, dan partisipasi sosial di era informasi.

Literasi Digital

United Nations Educational, Scientific and Cultural Organization (UNESCO) mendefinisikan literasi digital sebagai kemampuan untuk mengakses, mengelola, memahami, mengintegrasikan, mengkomunikasikan, mengevaluasi, dan menciptakan informasi secara aman dan tepat melalui teknologi digital untuk keperluan pekerjaan, pekerjaan yang layak, dan kewirausahaan. Berikut ini contoh implementasinya dalam kehidupan sehari-hari:

1. Kemampuan mengakses dan mengelola Informasi. Contohnya: Mahasiswa mencari artikel jurnal di Google Scholar, lalu menyimpan referensinya dengan benar untuk tugas akhir.
2. Kemampuan memahami dan mengintegrasikan Informasi. Contohnya: Seorang ibu rumah tangga memahami perbedaan antara berita kesehatan asli dan *hoaks* vaksin dari media sosial, lalu berdiskusi dengan posyandu setempat.
3. Kemampuan berkomunikasi secara digital. Contohnya: ASN di kecamatan mengirim laporan dalam bentuk Google Form dan rapat virtual dengan Zoom tanpa tergantung ke operator.
4. Kemampuan mengevaluasi dan menggunakan informasi dengan aman. Contohnya: Remaja tahu bahwa membagikan NIK dan foto KTP di media sosial itu berbahaya. Seorang guru tidak mengklik tautan mencurigakan di email atau di pesan WA dari nomor tidak dikenal dan memahami apa itu *phishing*.

5. Kemampuan menciptakan Konten Digital. Contohnya: Seorang nelayan membuat video edukasi tentang cara menangkap ikan ramah lingkungan dan mengunggahnya ke YouTube.

Framework Literasi Digital

UNESCO telah menetapkan Digital Literacy Global *Framework* (DLGF) sebagai kerangka kerja atau *framework* global dan di indonesia banyak elemen dalam Gerakan Nasional Literasi Digital (GNLD Siberkreasi), Guru Penggerak, dan Merdeka Belajar yang sejalan dengan DLGF. Dalam konteks Indonesia saat ini, DLGF dapat menjadi pendukung strategis bagi kebijakan pendidikan yang mengedepankan pendekatan pembelajaran berbasis pemahaman mendalam (*deep learning*).

Berikut ini adalah 3 level kompetensi literasi digital yang terdapat dalam DLGF:

1. Level Dasar
   Level ini berfokus pada kemampuan fungsional minimal agar seseorang bisa berpartisipasi secara digital. Sasarannya adalah siswa SD, pemula digital, dan masyarakat yang baru berkenalan dengan teknologi. Karakteristiknya adalah:
   a. Dapat mengoperasikan perangkat digital (HP, komputer, tablet).
   b. Mengakses internet, membuka aplikasi dasar (*browser*, email, WhatsApp).
   c. Menggunakan media sosial secara pasif (membaca, menyukai, menonton).
   d. Belum mampu mengevaluasi validitas informasi atau menjaga keamanan data.
2. Level Menengah

Mewakili pengguna digital yang mandiri dan efisien, namun belum sampai pada kemampuan tingkat tinggi atau strategis. Sasarannya adalah mahasiswa, guru dan tenaga kerja profesional, masyarakat digital aktif. Masyarakat digital aktif merujuk pada kelompok individu yang tidak hanya menjadi pengguna pasif teknologi digital, tetapi telah terlibat secara rutin, sadar, dan produktif dalam aktivitas digital yang memengaruhi kehidupan mereka sehari-hari—baik untuk informasi, komunikasi, pekerjaan, pembelajaran, hingga kontribusi sosial. Karakteristiknya adalah:

a. Mampu mengevaluasi dan membandingkan sumber informasi digital.
b. Menggunakan aplikasi digital untuk kerja kolaboratif (Google Docs, Zoom, LMS).
c. Membuat konten dasar: presentasi, infografis, video sederhana.
d. Mengelola privasi akun, menghindari *hoaks*, memahami etika digital.
e. Mampu menyelesaikan masalah teknis ringan (misalnya, troubleshooting koneksi, update *software*).

3. Level Mahir

Level ini diperuntukkan bagi pengguna yang inovatif, reflektif, dan produktif secara digital, serta mampu membimbing orang lain, menjadi pemecah masalah kompleks, pencipta solusi digital inovatif, dan agen perubahan digital di lingkungannya. Sasarannya adalah trainer, dosen, profesional bidang digital, *content* creator edukatif, tim IT, instruktur vokasi, desainer pembelajaran digital. Karakteristiknya adalah:

a. Menciptakan konten multimedia kompleks (e.g., video interaktif, produk *e-learning*, coding dasar)
b. Mampu mengelola proyek berbasis teknologi dan tim virtual.
c. Mengintegrasikan digital tools ke dalam pekerjaan dan proses pembelajaran.
d. Menjadi pendidik atau pelatih literasi digital bagi orang lain.
e. Peka terhadap isu global terkait AI, data ethics, dan jejak digital.
f. Menyelesaikan masalah tingkat tinggi, misalnya otomasi proses kerja, audit keamanan digital.

Ancaman dalam Literasi Digital

Literasi digital bukan hanya soal kecakapan teknis menggunakan gawai atau aplikasi, tetapi juga mencakup kemampuan memahami, mengevaluasi, dan menavigasi informasi serta teknologi secara etis dan kritis. Tanpa bekal literasi digital yang memadai, masyarakat rentan terjebak dalam konten palsu seperti deepfake, menjadi korban polarisasi akibat algoritma media sosial, serta tergelincir pada ketergantungan teknologi yang mengikis kemampuan berpikir reflektif.

Berikut ini empat ancaman yang terdapat dalam literasi digital:

1. Deepfake dan Manipulasi Digital
   Kemajuan teknologi kecerdasan buatan (AI) memungkinkan pembuatan deepfake—video atau suara yang tampak otentik tetapi sepenuhnya palsu. Masyarakat tanpa kecakapan literasi digital kritis akan mudah percaya pada konten palsu yang menghasut atau

menyesatkan. Contohnya, menjelang pemilu, beredar video "pidato" tokoh politik terkenal yang ternyata hasil manipulasi deepfake, memicu perdebatan dan kerusuhan digital.

2. Algoritma dan Polarisasi Informasi
   Platform seperti YouTube, TikTok, Instagram, dan Facebook menggunakan algoritma untuk menyajikan konten sesuai minat pengguna. Ini menciptakan *filter bubble* dan echo chamber, di mana pengguna hanya melihat perspektif yang memperkuat keyakinan sendiri, memicu polarisasi opini. Contohnya, seseorang yang menonton konten politik konservatif akan terus disuguhi konten serupa, membuatnya sulit melihat sudut pandang berbeda.
3. Ketergantungan Teknologi dan Krisis Daya Pikir
   AI, chatbot, dan *search engine* membuat akses informasi sangat cepat—tapi juga dapat membuat pengguna malas berpikir kritis. Ketergantungan berlebihan membuat generasi muda kurang mengasah logika, kreativitas, dan kemandirian berpikir. Contohnya, Mahasiswa mengandalkan ChatGPT untuk menjawab soal esai tanpa memahami isinya, bahkan menyalin mentah tanpa interpretasi.
4. Etika Digital dan Keamanan Siber
   Di dunia digital, banyak pelanggaran terjadi karena minimnya pemahaman etika dan keamanan digital dasar. Banyak pengguna tidak menyadari bahwa menyebarkan *hoaks*, mencuri data, atau meretas akun orang lain adalah tindakan melanggar hukum. Contohnya, remaja membobol akun Instagram temannya untuk "iseng", tanpa memahami konsekuensi hukum dan etikanya. Di

sisi lain, rendahnya kesadaran akan keamanan data membuat masyarakat rentan terhadap serangan siber seperti *phishing* (penipuan berbasis link/email), *malware*, pencurian identitas, dan eksploitasi data pribadi.

Jenis-Jenis Serangan Siber

Serangan siber adalah berbagai bentuk serangan digital yang ditujukan untuk mencuri data, merusak sistem, atau mengganggu layanan digital. Bentuknya meliputi *phishing*, *malware, ransomware,* hingga kebocoran data pribadi. Bahayanya sangat serius: pencurian identitas, pemerasan, peretasan akun keuangan, hingga lumpuhnya layanan publik seperti rumah sakit atau imigrasi.

Berikut ini jenis-jenis serangan siber yang sering terjadi dalam kehidupan sehari-hari baik secara individu maupun organisasi:

1. *Phishing*

   Phishing adalah upaya penipuan digital dengan cara menyamar sebagai pihak terpercaya (seperti bank, instansi resmi, atau layanan populer) untuk memancing korban agar memberikan informasi sensitif seperti:

   a. Username dan password
   b. Nomor kartu kredit
   c. Kode OTP
   d. Data pribadi (NIK, tanggal lahir, dan lain-lain)

   Ciri-ciri *phishing*:

   a. Email atau pesan mencurigakan yang mendesak ("akun anda diblokir, segera klik link ini!")
   b. Link palsu yang mirip asli: bri-indonesia.co alih-alih bri.co.id

c. Lampiran berisi virus atau *malware*

2. *Social Engineering*

   Social Engineering adalah metode manipulatif yang mengeksploitasi kepercayaan, emosi, atau kelengahan manusia untuk mendapatkan akses ke sistem atau informasi. Jika *phishing* menipu lewat teknologi, maka *Social Engineering* menipu lewat psikologi. Jenis-jenis *Social Engineering*:

   a. *Pretexting*: Penipu berpura-pura jadi petugas resmi yang butuh data.
   b. *Baiting*: Menawarkan hadiah atau bonus palsu (misal: "menang undian").
   c. *Quid pro quo*: Menjanjikan bantuan atau layanan palsu sebagai imbalan informasi.
   d. *Tailgating*: Mengikuti orang ke area terbatas (di kantor, lab komputer, dan lain-lain.

   Data tersebut kemudian dijual di dark web atau website forum yang sering diakses oleh member jaringan sindikat tertentu.

3. Kebocoran data pribadi

   Kebocoran data pribadi (*data breach*) terjadi ketika informasi sensitif seseorang diakses, disalin, atau disebarluaskan tanpa izin, baik karena peretasan, kelalaian sistem, maupun manipulasi manusia.

   Informasi yang bisa bocor meliputi:

   a. Identitas pribadi: NIK, nama lengkap, tanggal lahir
   b. Kontak pribadi: email, nomor telepon, alamat rumah
   c. Data finansial: nomor rekening, kartu kredit, gaji
   d. Data medis: riwayat penyakit, BPJS

e. Akun digital: username, password, history aktivitas

Mengapa data yang bocor ini bisa berbahaya? Sebab bisa digunakan untuk:

a. Penipuan identitas (*identity theft*)
b. Pembobolan akun bank atau dompet digital
c. Penyebaran *hoaks* atau fitnah pakai nama anda
d. Pemerasan (*blackmail*) berbasis data sensitif
e. Pemalsuan dokumen hukum/keuangan

4. *Malware*

Malware (*malicious software*) adalah perangkat lunak berbahaya yang dirancang untuk merusak sistem komputer atau perangkat, mencuri data, memata-matai aktivitas pengguna, mengambil alih kendali perangkat. Jenis-jenis *malware*:

a. Virus: Menyebar lewat file yang dijalankan
b. Worm: Menyebar otomatis tanpa bantuan pengguna
c. Trojan: Menyamar sebagai aplikasi aman (contoh: "aplikasi diskon" tapi ternyata mencuri data)
d. Spyware: Merekam aktivitas pengguna diam-diam
e. Adware: Menampilkan iklan berlebihan yang sering disusupi virus

5. Ransomware

Ransomware adalah jenis *malware* yang mengunci atau mengenkripsi data korban, lalu pelaku meminta tebusan (ransom) agar data bisa diakses kembali.

Ciri-ciri ransomware adalah tiba-tiba file-file penting tidak bisa dibuka, muncul pesan "file anda telah dikunci". Lalu muncul perintah untuk mengirimkan sejumlah uang untuk membuka akses. Tebusan biasanya diminta dalam

bentuk kripto seperti bitcoin, etherium, atau litecoin.

Teknik Pengamanan Siber

Menjawab berbagai persoalan siber kita setidaknya membutuhkan beberapa teknik pengamanan siber yang bis akita praktekkan agar tidak menjadi korban kejahatan siber terserbut. Berikut ini teknik pengamanan tersebut.

1. Enkripsi Data
   Enkripsi data adalah proses mengubah informasi asli (*plaintext*) menjadi bentuk yang tidak bisa dibaca (*ciphertext*) tanpa kunci khusus. Tujuannya adalah melindungi data dari akses oleh pihak yang tidak berwenang, baik saat data sedang disimpan (*data-at-rest*) maupun saat sedang dikirim (*data-in-transit*).
2. *Password hygiene*
   Password hygiene adalah praktik menjaga keamanan akun digital dengan cara:
   a. Menggunakan kata sandi yang kuat: kombinasi huruf besar, kecil, angka, dan simbol (misal: G4ruda#2025)
   b. Tidak memakai kata sandi yang sama di banyak akun
   c. Menghindari data pribadi (nama, tanggal lahir) sebagai password
   d. Mengganti password secara berkala
   e. Tidak membagikan password kepada siapa pun, bahkan orang dekat
3. *Two-Factor Authentication* (2FA)
   Two-Factor Authentication (2FA) adalah sistem keamanan berlapis dua yang meminta verifikasi tambahan selain password. Selain password kita akan

diminta mengisi kode OTP yang telah kita terima via SMS/email, atau verifikasi lewat aplikasi autentikator (misal *Google Authenticator*), atau gunakan sidik jari/wajah (biometrik). Jika password bocor, akun tetap tidak bisa diakses tanpa verifikasi kedua. Hal ini akan melindungi akun dari peretasan, bahkan jika pelaku tahu sandinya.

Literasi Digital Masa Depan

Kita dapat menjadi sukses baik sebagai individu maupun organisasi jika mampu mencuri start dalam menguasai kemampuan literasi digital masa depan. Misalnya saja AI, *Metaverse*, big data, dan *Internet of Things* bukan lagi konsep futuristik, melainkan sudah aktif membentuk cara belajar, bekerja, dan berinteraksi sosial kita selama ini. Siapa yang siap lebih dulu, akan jadi pelaku utama, bukan korban disrupsi.

Lalu, apa saja kemampuan literasi masa depan tersebut? Berikut di antaranya:

1. Literasi Kecerdasan Buatan (*AI Literacy*)
   Mahasiswa dan pelajar masa depan harus mampu memahami cara kerja algoritma AI, etika penggunaannya, serta mengantisipasi bias dan disinformasi yang dapat muncul dari sistem otomatisasi seperti ChatGPT, Google Gemini, dan rekomendasi konten media sosial.
2. Literasi *Metaverse* dan Ruang Virtual
   Interaksi di ruang *Metaverse* dan *Augmented Reality* akan menjadi bagian integral dari kehidupan sosial dan ekonomi. Maka diperlukan literasi visual, pengelolaan identitas digital lintas *platform*, dan pemahaman terhadap hak-hak digital di ruang virtual. Ini mencakup

interaksi melalui avatar, pemanfaatan VR/AR (*Virtual & Augmented Reality*), serta kesadaran terhadap identitas digital, keamanan, dan etika di ruang maya

3. Literasi Data dan Pemikiran Berbasis Bukti
   Kemampuan membaca data, mengenali pola, memahami grafik dan tren, serta membuat keputusan berbasis bukti menjadi kompetensi wajib di era big data. Literasi digital masa depan akan menyatu dengan numerasi dan sains. Kemampuan ini secara spesifik adalah untuk membaca, menganalisis, dan memaknai data dalam berbagai bentuk—angka, grafik, tabel, infografik, maupun statistik—lalu menggunakannya untuk mengambil keputusan yang logis, objektif, dan berbasis bukti nyata (*evidence-based reasoning*).

Daftar Pustaka

Bawden, D. (2008). Origins and concepts of digital literacy. In C. Lankshear & M. Knobel (Eds.), Digital Literacies: Concepts, Policies and Practices (pp. 17–32). Peter Lang.

Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. Luxembourg: Publications Office of the European Union.

Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. Journal of Educational Multimedia and Hypermedia, 13(1), 93–106.

Hargittai, E., & Litt, E. (2013). New strategies for internet skills: Exploring the digital literacy divide. Information, Communication & Society, 16(2), 197–216.

Helsper, E. J., & Eynon, R. (2010). Digital natives: Where is the evidence? British Educational Research Journal, 36(3), 503–520.

Hobbs, R. (2010). Digital and media literacy: A plan of action. Washington, DC: Aspen Institute.

Kemenkominfo. (2022). Gerakan Nasional Literasi Digital #SiBerkreasi. https://siberkreasi.id

McGrew, S., Breakstone, J., Ortega, T., Smith, M., & Wineburg, S. (2018). Can students evaluate online sources? Learning

from assessments of civic online reasoning. Theory & Research in Social Education, 46(2), 165–193.

Ng, W. (2012). Can we teach digital natives digital literacy? Computers & Education, 59(3), 1065–1078.

Nisa, U., Nisak, C. L. C., & Fatia, D. (2023). Literasi digital lansia pada aspek digital skill dan digital safety. Jurnal Komunikasi Global. Link.

Silvester, S., Saputro, T. V. D., & Manggu, B. (2024). Pendampingan literasi digital bagi guru sekolah dasar dalam mengimplementasikan Kurikulum Merdeka. Lumbung Inovasi. Link.

Suherman, A., Supriyadi, T., & Safari, I. (2020). Promoting digital literacy skills: An action research to people of Kampung Literasi. Universal Journal of Educational Research, 8(4), 1372–1386. Link.

UNESCO. (2018). Digital Literacy Global Framework. Paris: United Nations Educational, Scientific and Cultural Organization.

Wilson, C. (2012). Digital and media literacy: Connecting culture and classroom. Cambridge, MA: Harvard University Press.

Tentang Penulis

Daniel Pandapotan, S.Sos., M.IP, adalah dosen di program studi ilmu perpustakaan dan sains informasi di Universitas Wijaya Kusuma Surabaya. Penulis memiliki fokus keilmuan dan penelitian di bidang ilmu informasi, teknologi media, dan teknologi pembelajaran. Buku ini adalah salah satu karya dan inshaa allah secara konsisten akan disusul dengan buku-buku berikutnya. Pokok bahasan buku yang ditulis semata-mata untuk berbagi ilmu pengetahuan.

Buku Literasi Digital: Teori, Praktik, dan Tantangan hadir sebagai panduan menyeluruh untuk memahami dan menguasai literasi digital di era teknologi yang terus berkembang. Buku ini menguraikan konsep dasar literasi digital, ancaman dunia siber, hingga strategi pengamanan informasi digital. Pembaca juga akan diajak mengeksplorasi berbagai pilar literasi digital, peran pentingnya dalam kehidupan sehari-hari, serta tantangan dan solusi dalam menghadapi perubahan digital yang dinamis. Selain membahas teori, buku ini menekankan penerapan literasi digital dalam konteks nyata, termasuk pemanfaatan teknologi seperti Artificial Intelligence (AI), Internet of Things (IoT), media sosial, dan e-learning. Isu-isu kontemporer seperti fake news, cyberbullying, keamanan data, dan etika digital juga dibahas secara kritis. Setiap bab disusun untuk memberikan pemahaman yang aplikatif, lengkap dengan studi kasus dan tips praktis bagi pembaca dari berbagai kalangan—terutama pendidik, pelajar, dan masyarakat umum. Dengan pendekatan interdisipliner dan konten yang relevan, buku ini menjadi sumber belajar penting untuk membangun kesadaran digital yang cerdas, bijak, dan bertanggung jawab. Buku ini tidak hanya mengajarkan cara menggunakan teknologi, tetapi juga mengasah kemampuan berpikir kritis, memahami hak dan kewajiban digital, serta membentuk karakter dalam menghadapi dunia digital yang kompleks.

DITERBITKAN OLEH
PT. MIFANDI MANDIRI DIGITAL

Jln Payanibung Ujung D
Dalu Sepuluh-B, Tanjung Morawa
Kab. Deli Serdang Sumatera Utara

ISBN 978-634-7226-24-2
9 786347 226242