



SCHOOLTOOL USER GROUP

Security: Who Can See What?

Practical security, smart access, and a clearer way to review rights

SECURITY

PRIVACY

SCHOOLTOOL

Today's route

Two stops, one goal: access that makes sense.

1

Security in plain English

- What security means in schools
- PII and privacy
- Everyday best practices
- Incident response + reporting timelines

WHY IT MATTERS

2

SchoolTool in practice

- Users, groups, rights, and scope
- Least privilege
- Who has what?
- Reports, exports, and review routines

HOW TO REVIEW IT

Security in plain English

It is less about “cyber stuff” and more about deliberate access.

Security = protecting information and systems from access, change, loss, or disruption that should not happen.

WHO

gets an account?

WHAT

can they see?

DO

they need to edit?

WHEN

**does access
change?**

Security is not just an IT thing

Good security happens where people, process, and technology overlap.



Three related ideas — not the same thing

SchoolTool sits where security, privacy, and cybersecurity meet.



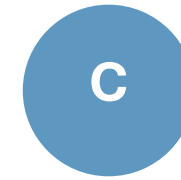
SECURITY

Protecting information and systems from unauthorized access, changes, loss, or disruption.



PRIVACY

Using, collecting, and sharing personal information appropriately — even when access is technically possible.



CYBERSECURITY

Applying security practices to digital accounts, devices, networks, systems, and data.

The three-question security check

A simple way to test whether access and information are protected.

1

**Can the right people
see it?**

CONFIDENTIALITY

2

**Is the information
accurate?**

INTEGRITY

3

**Can authorized
people get to it?**

AVAILABILITY

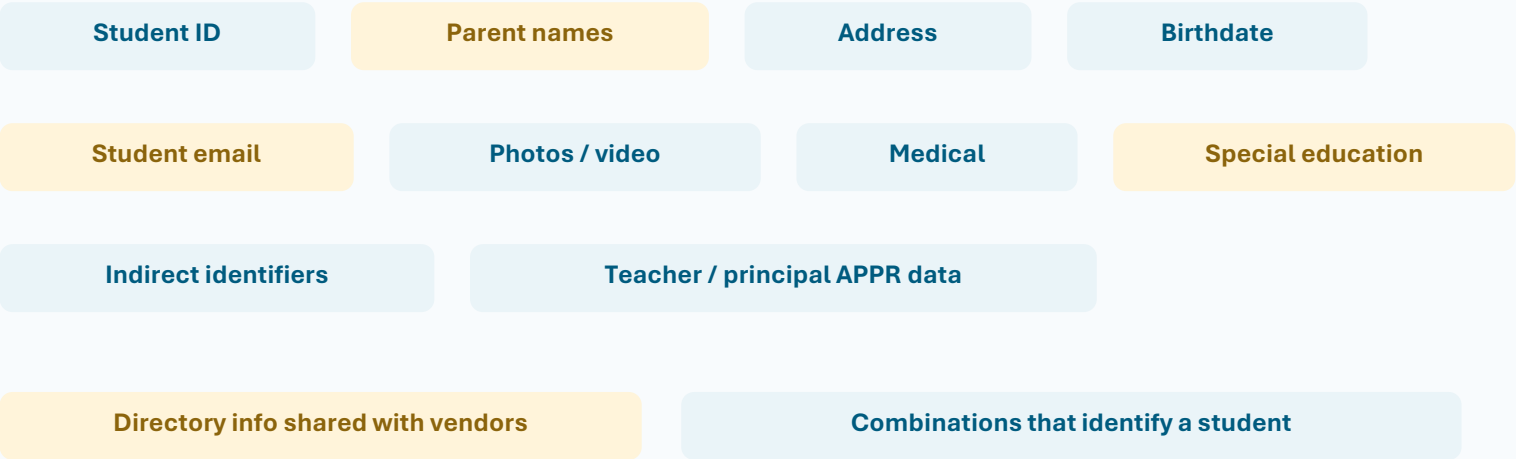
PII is more than a student name

Protected information can identify a student directly — or when pieces are combined.



Student record

Think beyond “secret.”
Ask: Is it protected, and am I handling it appropriately?



Education Law 2-d uses the FERPA definition of student PII and also protects certain teacher/principal APPR information.

The rules behind the routines

Education Law 2-d + Part 121 turn privacy and security into ongoing district responsibilities.

1

PII
Protect confidentiality

2

PARENTS
Bill of Rights

3

POLICY
Data security +
privacy

4

NIST
Use a cybersecurity
framework

5

VENDORS
Third-party contracts

6

TRAINING
Annual employee
training

7

INCIDENTS
Reporting +
notification

8

DPO
Data Protection
Officer

These are governance tasks — not just annual compliance tasks.

Small habits. Big protection.

Most security improvement happens in ordinary moments.

EMAIL

Pause before clicking

Verify sender, context, and links.

PASSWORDS

Make them unique

Use strong passphrases; do not share them.

MFA

Add another layer

A stolen password should not be enough.

DATA

Use approved places

Share PII only with approved users/systems.

DEVICES

Protect the device

Lock, encrypt, and avoid risky connections.

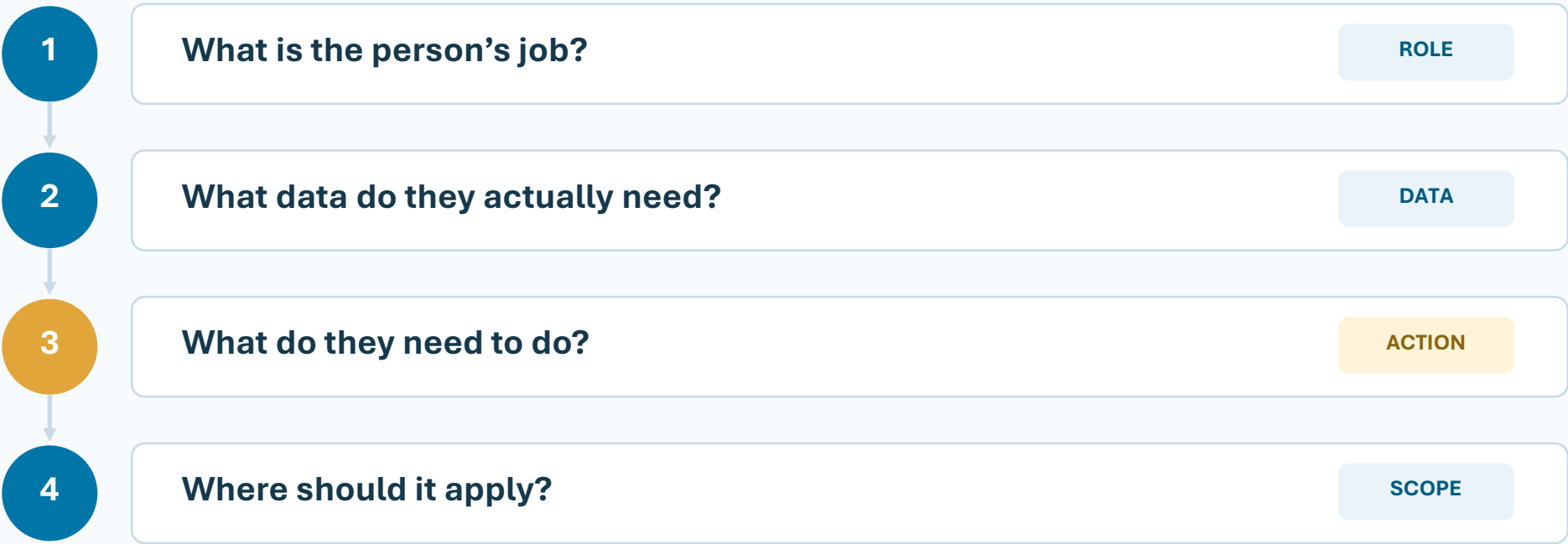
AI

Pause before pasting

Do not enter PII without district approval.

Least privilege = enough, not everything

Give people what they need for the job — then stop.

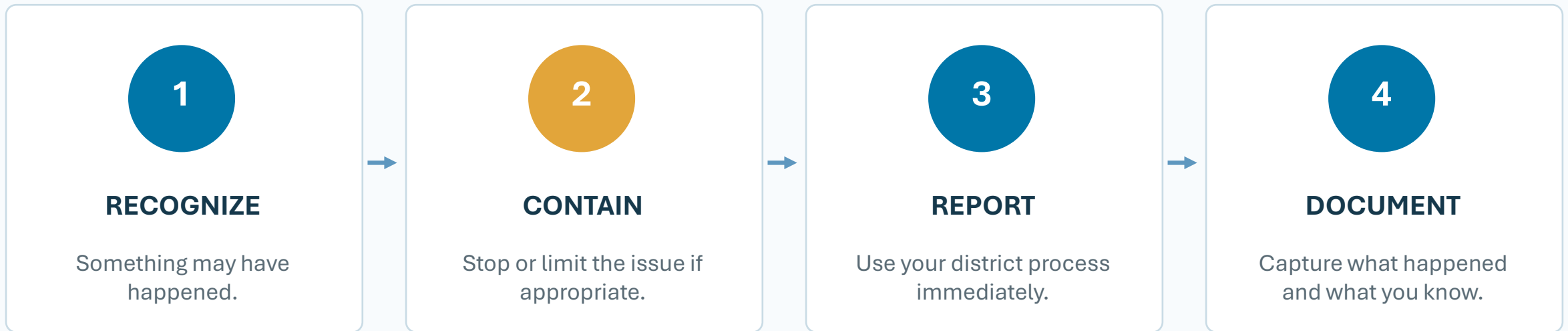


**JUST
ENOUGH**

Access
should be
explainable.

Uh-oh. Now what?

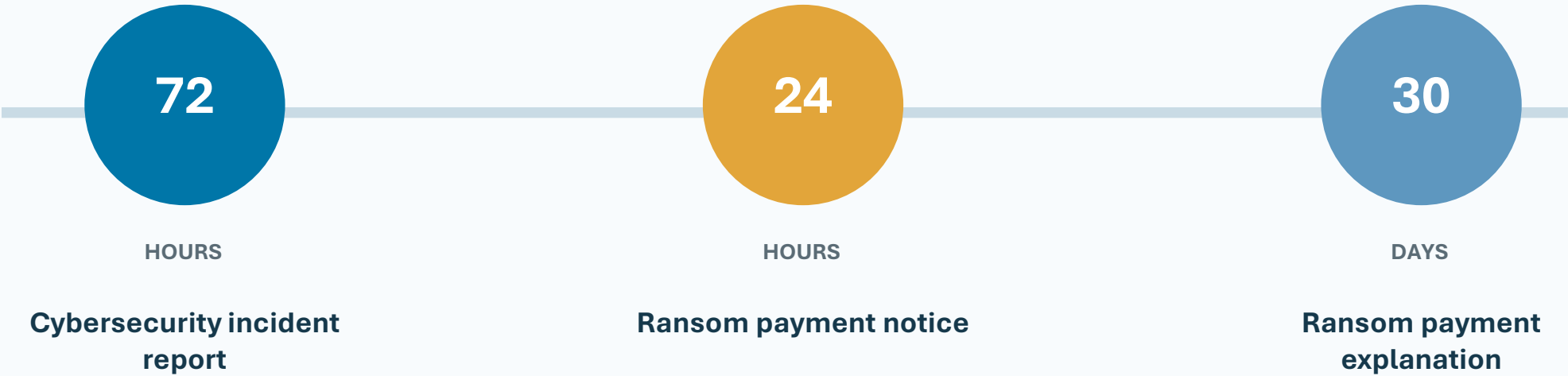
When something looks wrong, a simple response is easier to remember.



If you are unsure, report the concern — do not wait for certainty.

When the clock matters

Article 19-C adds state reporting requirements for cybersecurity incidents and ransom payments.



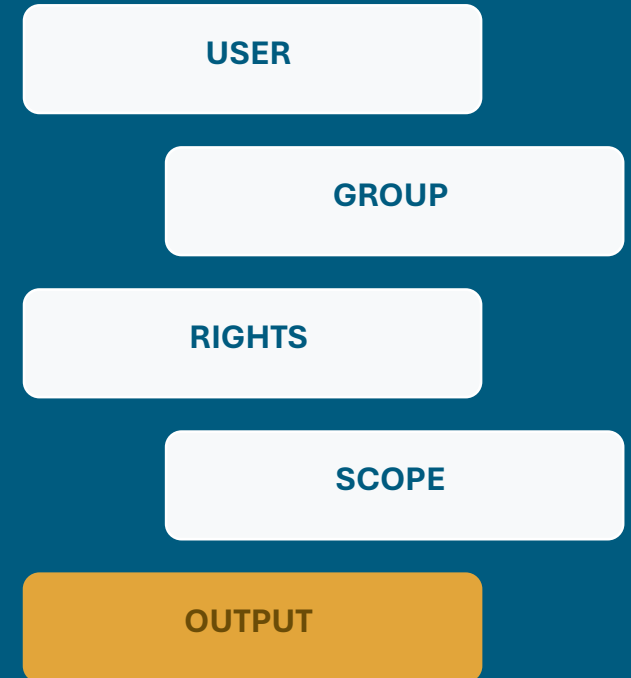
Local takeaway: report concerns through your district process quickly so the right people have time to respond.

02

SCHOOLTOOL IN PRACTICE

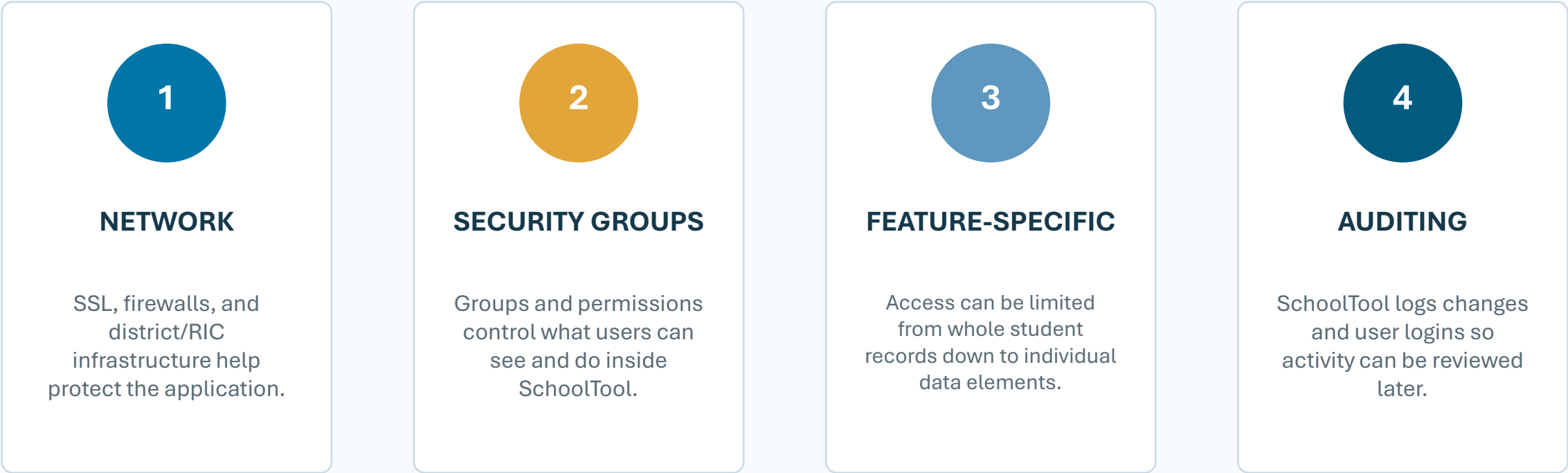
From policy to permissions

Users → Groups → Rights → Scope → Outputs



SchoolTool security has multiple layers

The application provides safeguards — districts still decide who gets access and how broad it should be.



SchoolTool is one layer of the district’s overall security posture — not the entire posture.

Who are you? What can you do?

SchoolTool treats authentication and authorization as two separate steps.



AUTHENTICATION

“Who are you?”

Local login • Active Directory • Google • Microsoft • MFA



AUTHORIZATION

“What are you allowed to do?”

Group membership → Security Tree permissions → access
inside SchoolTool

SchoolTool supports multiple authentication paths

A district can use more than one login method at the same time.

authentication method. Each section can be expanded to view additional

SchoolTool Authentication (Local User Accounts) ✓

On-Premise Active Directory (Network Accounts) ✓

Google SSO ✓

Microsoft 365 (Without Azure Active Directory) ✓

Microsoft Azure Active Directory ✓

Current SchoolTool authentication choices

LOCALON-PREM AD

GOOGLE SSGOOGLE SSO

MICROSOFT 365MICROSOFT 365

AZURE ADAZURE AD

Authentication verifies identity. The login method does not, by itself, define what the user can see in SchoolTool.

MULTIPLE METHODS CAN COEXIST

Who manages the group membership?

The answer depends on the authentication method.

MANAGED IN SCHOOLTOOL

Local SchoolTool accounts

Google SSO

Microsoft 365 without Azure AD

Local user groups map to SchoolTool security groups.

MANAGED EXTERNALLY

On-Premise Active Directory

Microsoft Azure Active Directory

Directory group membership determines the SchoolTool security groups assigned to the user.

Keep at least one local Admin account as an SSO fallback.

The Security Tree is where rights become real

SchoolTool permissions are assigned to security groups — then users inherit them through group membership.

Maintenance > User/Group > Groups and Security Tree

SchoolTool security groups:

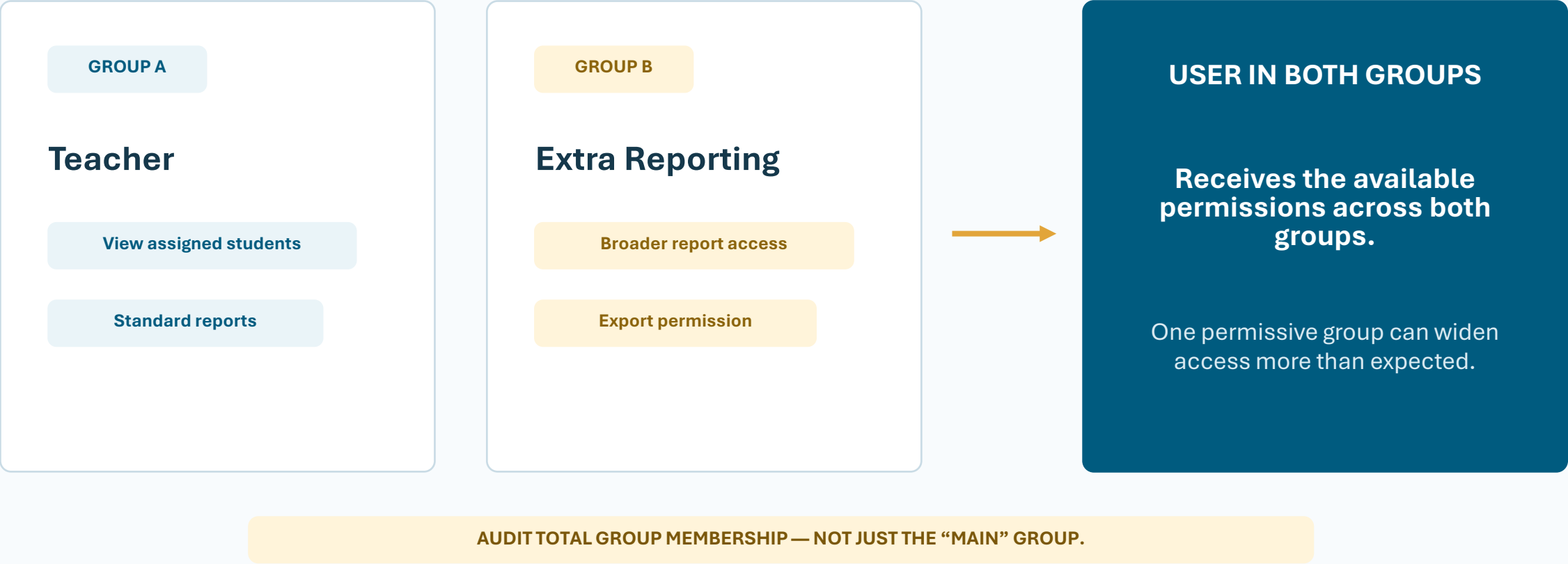
the green Add + button to create a new group (including all existing permission settings), unique and identifiable. If you're using an external directory, group names must match those user group names exactly.



- 1 Create or copy a clearly named security group.
- 2 SchoolTool recommends the “SMS_” naming convention.
- 3 External directory group names must match exactly.
- 4 **Expand the Security Tree and assign only the needed permissions.**
- 5 Save — and document what the group is for.

The rule that can surprise you

A user can belong to multiple groups — and SchoolTool uses the least restrictive permission set across them.



Build groups that are easy to explain and audit

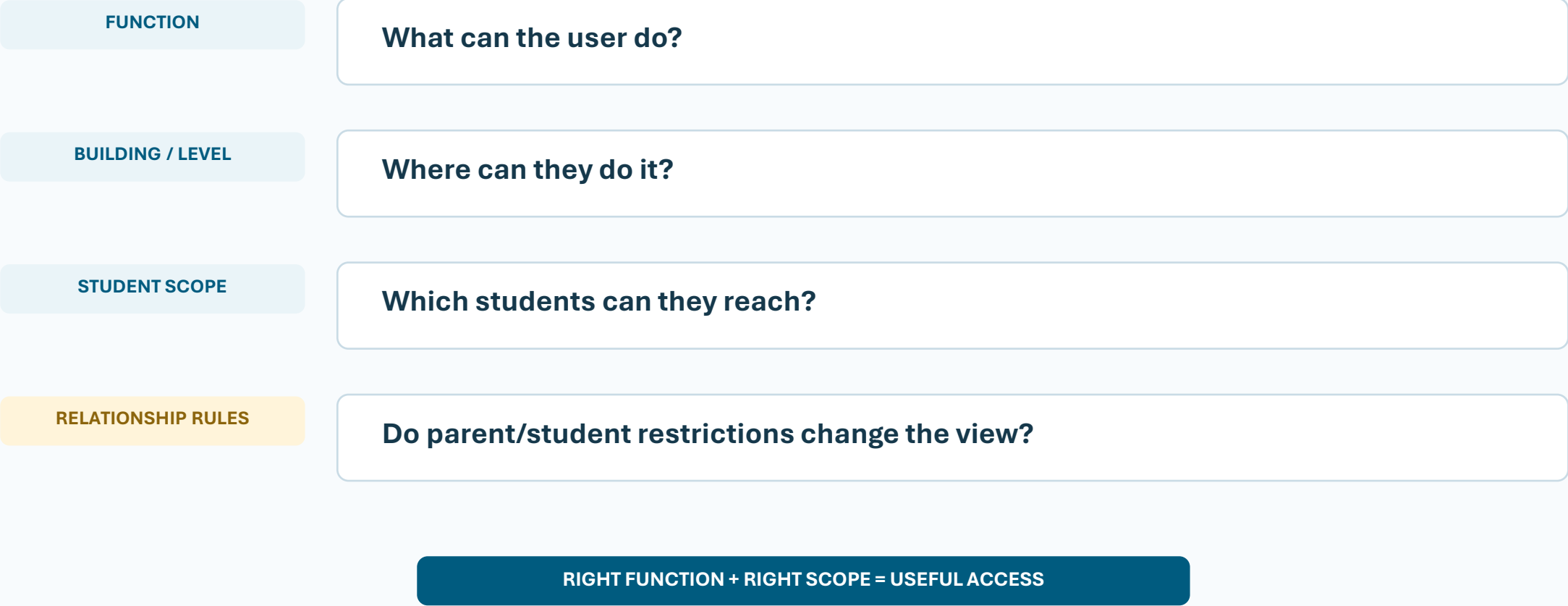
Role-based design works especially well when the names and purpose stay predictable.

SMS_TEACHER classroom	SMS_COUNSELOR caseload	SMS_NURSE health
SMS_SECRETARY office	SMS_ADMIN building	SMS_REPORTING targeted

SchoolTool can also use separate groups for different building/school-level permissions and for restricted vs. unrestricted parent access.

Scope is part of the security decision

The same functional right can be appropriate in one scope and too broad in another.



MFA: another layer at login

Mindex recommends MFA for all users; the available method depends on how the district authenticates.

GOOGLE / MICROSOFT / AZURE

Use the identity provider’s MFA / third-party MFA.

External MFA is Mindex’s preferred approach when available.

SCHOOLTOOL-PROVIDED MFA

Can add MFA to local accounts and some on-prem AD scenarios.

Email code: 6 digits • valid 15 minutes
• 3 attempts.

WHERE TO REQUIRE IT

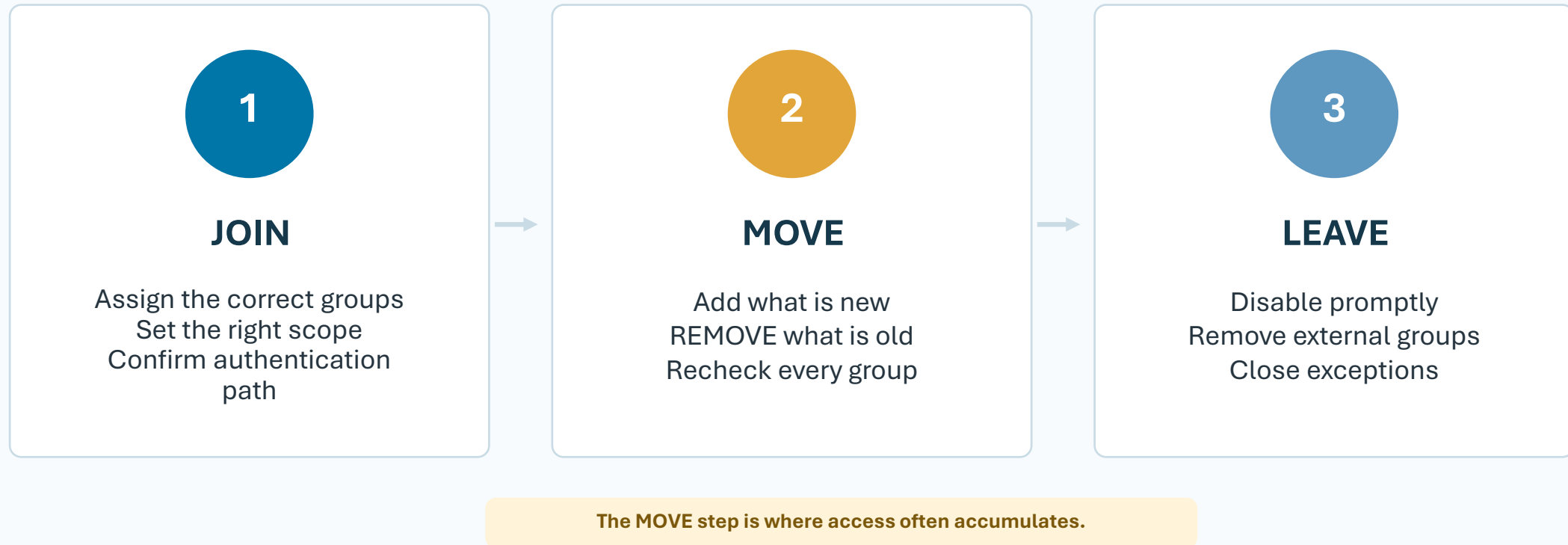
Maintenance > User/Group > Groups and Security Tree

Permission path: Login > Require MFA

Availability varies by authentication method and client.

Join. Move. Leave.

Access should follow the person's current role — not their employment history.



Some accounts deserve a brighter spotlight

The impact of incorrect access is not the same for every account.



PRIVILEGED / ADMIN

Keep the list small. Review often.
Use elevated access only when
needed.



BOCES / VENDOR / SUPPORT

Confirm the relationship is active
and the assigned groups are still
necessary.



SSO FALLBACK / SERVICE

Know why the account exists, who
owns it, and how it is protected.

The big question: Who has what?

Audit in both directions — group → users and user → groups.

GROUP → USERS

Pick a security group

- What permissions does it grant?
- Who is in it?
- Where is membership managed?
- Is the scope appropriate?

USER → GROUPS

Pick a person

- What groups are assigned?
- Which group creates each permission?
- Did access accumulate over time?
- Does the total picture match the job?

Two built-in reports answer two different questions

Both live at Maintenance > User/Group > Groups and Security Tree.

REPORT BY GROUP

What rights does this group have?

Lists the permissions assigned to each security group, sorted by group and then permission.

Group and Security Permissions	
<u>SMS Administrators</u>	Batch 3
Attendance/Attendance	Batch 3
Attendance/Attendance Policy	Batch 3
Attendance/Attendance Report	Batch 3
Attendance/Audit Reports	Batch 3
Attendance/Batch Make Present	Census
Attendance/Daily Attendance Mouse-overs	Census
Attendance/Daily Roster Report	Census
Attendance/Enter	Census
Attendance/Missed Classes Tab/Delete	Census
Attendance/Missed Classes Tab/Edit	Census
Attendance/Missed Classes Tab/Enter	Census

GROUP → PERMISSIONS

REPORT BY PERMISSION

Which groups have this right?

Lists the groups assigned to each individual permission, sorted by permission and then group.

Group and Security Permissions	
<u>Attendance/Attendance</u>	SMS_A
SMS_Website	SMS_A
SMS Administrators	SMS_A
SMS Attendance	SMS_A
SMS Counseling	SMS_C
SMS Curriculum	SMS_C
SMS Discipline	SMS_C
SMS HS CoordOffice	SMS_C
SMS Principal	SMS_C
SMS ScheduleAdmin	SMS_C
SMS SUPER	SMS_C
SMS TrainingCO	SMS_C
SMS TrainingElem	SMS_C

PERMISSION → GROUPS

Now answer: Who is in the group?

Account Maintenance provides the membership side of the review for local SchoolTool accounts.

Maintenance > User/Group > Account Maintenance

ACCOUNT MAINTENANCE

Filters:

Last Name Contains:

User Name Contains:

Locked Account:

☒ Ignore ☐ Locked ☐ Not Locked

Search

Choose an action for the selected accounts:

☐ Generate new password

☒ Automatically send em

☐ Delete account

☐ Unlock account

☐ Add account to selected group

Select One

☐ Remove account from selected group

Select One

Filter by last name, username, locked status — or one or more groups.

WHAT THIS LETS YOU DO

- Search for users in a selected group
- Review local account status
- Open an individual account
- Update group assignments
- Perform batch group operations

ACCOUNT MAINTENANCE

User name: frevans@yooohoo.com

☒ Generate new password

☒ Automatically send email to u

☐ Set password to

☐ Delete account

☒ Save group assignments

☐ SMS_Administrators

☒ SMS_Parents

☐ SMS_Students

☐ SMS_Teachers

USER ↔ GROUP MEMBERSHIP

A practical SchoolTool security audit

SchoolTool gives you the pieces — use them in a repeatable order.

1

Pick the sensitive right

Example: Discipline, Medical, Export, Maintenance

2

Run Report by Permission

Which security groups have that right?

3

Run Report by Group

What else does each of those groups grant?

4

Use Account Maintenance

Which local users belong to those groups?

5

Check the whole user

Other groups + scope + current job role

6

Reconcile + document

Confirm with HR / staffing / directory data

SUPPORTING TOOL

Custom Export > User can add context such as username, role, email, and building/school level — useful for reconciling access with current staffing. It is supporting context, not a direct permissions report.

SchoolTool already keeps an audit trail

Use the audit log to answer “who did what, when, and to whom?”

RECORD CHANGES

Student + faculty changes

The audit log records changes and shows the person who made the change, the date/time, and the record affected.

WHO • WHAT • WHEN • TO WHOM

USER LOGINS

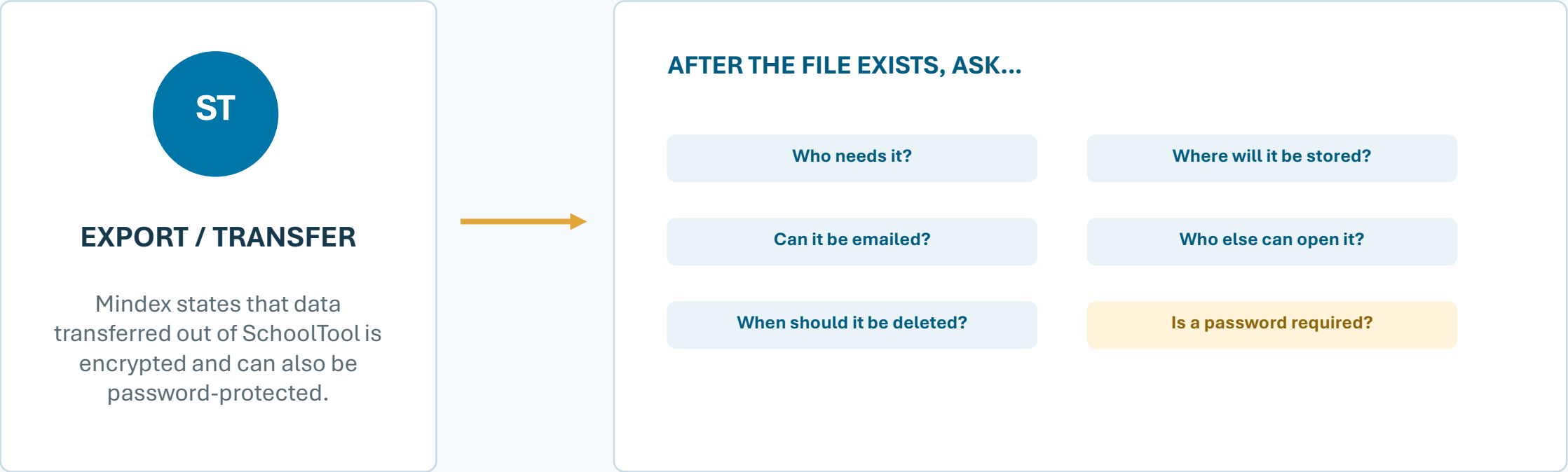
Login activity is audited too

SchoolTool records the user name plus the date, time, and IP address used to access the system.

USEFUL FOR FOLLOW-UP + INVESTIGATION

When data leaves SchoolTool

SchoolTool protects transfers — districts still need good handling practices after the file is created.



Make the decision visible

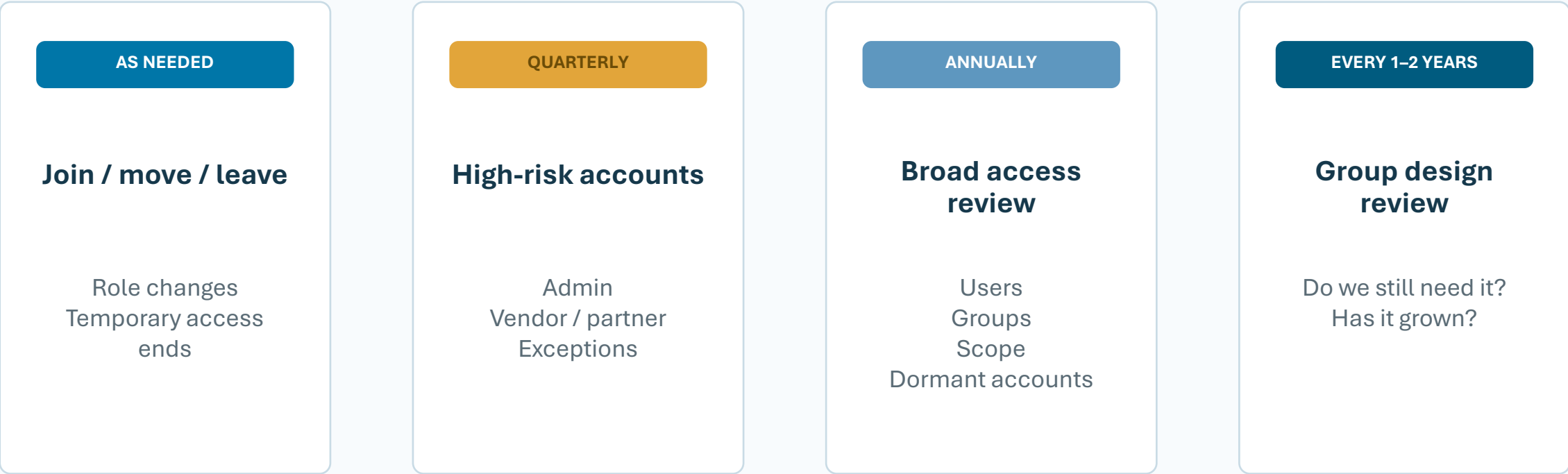
A simple access matrix turns “tribal knowledge” into a repeatable standard.

ROLE	SCHOOLTOOL?	BASE GROUP	EXTRA GROUPS	SCOPE	OWNER
MS Teacher	Yes	SMS_Teacher	—	Assigned students	HR / IT
Counselor	Yes	SMS_Counselor	As needed	Caseload / building	Program lead
Vendor	Sometimes	Support	Limited only	Defined task	IT / RIC

The matrix is the expectation. SchoolTool is the reality you audit against.

Security is a routine, not a cleanup project

Attach reviews to predictable moments so access does not quietly accumulate.



Scenario: the access that followed someone

A role changed six months ago. The old access did not.

A former middle-school secretary moved to a district-office role. Today, they can still open middle-school discipline information.

1

Which groups are they in now?

2

Run Report by Group: what do those groups grant?

3

Run Report by Permission: which group grants Discipline?

4

Where is the membership managed?

5

What does the audit trail show?

6

What process failed?

Fix the account — then fix the process.

Seven things worth remembering

The SchoolTool details reinforce the same security principles.

- 1 Authentication is not authorization** Login method and access rights are separate.
- 2 Groups drive permissions** The Security Tree is where rights are configured.
- 3 Multiple groups can widen access** Audit the user's total group membership.
- 4 Use both built-in security reports** Group → permissions and permission → groups.
- 5 Account Maintenance shows membership** Use it to find local users in selected groups.
- 6 Audit logs are your trail** Use them for changes, logins, and follow-up.
- 7 Make review routine** Access should change when the job changes.

The safest access is access you can explain in one sentence.

What is working in your district?

How are you reviewing users, groups, rights, reports, audit logs, and exports?

?

**Are you using Report by
Group / Permission?**

?

**How are you reviewing
group membership?**

?

**What part of access review
is hardest?**

Key references: Mindex Groups and Security Tree • Account Maintenance • SchoolTool Authentication • Creating SchoolTool Security Groups • SchoolTool Security Overview • RIC One Data Privacy & Security materials • NYS Education Law 2-d / Part 121 • NYS General Municipal Law Article 19-C



Eastern Suffolk BOCES Board and Administration

President

Lisa Israel

Vice President

Robert P. Sweeney

Members

Arlene Barresi
Angelo Cassarino
Linda S. Goldsmith
William Hsiang

Kelli Anne Jennings
Susan Lipman
Joseph LoSchiavo
Anne Mackesey
James F. McKenna

Brian O. Mealy
Victoria Molloy
Catherine M. Romano
John Wyche

District Superintendent

Jasmin Varela, Ed.D.

Chief Operating Officer

David Wicks

Associate Superintendent

Claudy Damus-Makelele - Educational Services

Associate Superintendent

Katelyn Fretto - Management Services

Assistant Superintendent

Vacant - Human Resources

Directors

Christopher Carlos - Business Services
Heather H. Ciccone - Regional Information Center
Arlene Durkalski - Human Resources
Barbara Egloff - Career, Technical and Adult Education
Krystle M. Hernandez-Barnett, Ed.D. - Educational Support Services
Ryan Jacobellis - Facilities
Gina Reilly - Special Education
Elaine Romeyk - Administrative Services
Jachan Watkis - Diversity, Equity, and Inclusion

www.esboces.org

Eastern Suffolk BOCES does not discriminate against any employee, student, applicant for employment, or candidate for enrollment on the basis of sex, gender, race, color, religion or creed, age, weight, national origin, marital status, disability, sexual orientation, gender identity or expression, transgender status, military or veteran status, domestic violence victim status, genetic predisposition or carrier status, or any other classification protected by Federal, State, or local law. This policy of nondiscrimination includes: access by students to educational programs, student activities, recruitment, appointment and promotion of employees, salaries, pay, and other benefits. ESBOCES also provides equal access to the Boy Scouts and other designated youth groups. ESBOCES fully complies with all applicable rules and regulations pertaining to civil rights for students and employees (e.g., Title IX of the Education Amendments of 1972, §504 of the Rehabilitation Act of 1973, Titles VI and VII of the Civil Rights Act of 1964, Dignity for All Students Act, §303 of Age Discrimination Act of 1975, the Americans with Disabilities Act of 1990, and the Boy Scouts of American Equal Access Act of 2001). Inquiries regarding the implementation of the above laws should be directed to either of the Eastern Suffolk BOCES Civil Rights Compliance Officers at ComplianceOfficers@esboces.org: the Assistant Superintendent for Human Resources, 631-687-3029, or the Associate Superintendent for Educational Services, 631-687-3056, 201 Sunrise Highway, Patchogue, NY 11772. Inquiries may also be addressed to the Office for Civil Rights at the US Department of Education, 32 Old Slip, 26th Floor, New York, NY 10005, 646-428-3800, OCR.NewYork@ed.gov.