



ManageBac+

by **faria**
Education Group

Leadership Resource

The Vendor Vetting Checklist for School Leaders

By Sibylle Harth

Director of Teaching, Learning & Technology
International School of Düsseldorf

A practical companion to
Cultivating a Responsible
Digital Ecosystem.

A structured set of
questions to ask before
any digital tool takes root
in your school — covering
both educational and
operational systems.

This checklist includes:

- Before adoption
- Additional considerations
- During pilot
- Ongoing review

managebac.com



How to Use This Checklist

No tool is perfect on every dimension, and the goal is not to score it out of twenty. This is a structured conversation — between leadership, IT, the Data Protection Officer, and the educators or operational leads championing the tool. Work through it together before a tool becomes embedded; the questions get harder to answer once data starts flowing.

The checklist applies to systems across the school such as teaching and learning platforms, but also operational systems such as admissions, HR, finance and communication, which often process significant volumes of personal data.

1

Before adoption

Preparing the soil.
The questions that decide whether something should take root at all — moving from purpose, to data and risk, to technical safeguards, to formal sign-off.

☐

Is the purpose of the tool clear and documented (educational or operational)?

What problem are we solving, and who decided this was the right way to solve it? “A teacher is enthusiastic” is a starting point, not a justification. The same applies to operational systems: a department's preference is not, on its own, a basis for adoption.

☐

Does it duplicate or overlap with something we already have?

Map it against the existing stack before adding to it. Overlap creates confusion, fragmented data, and avoidable subscription cost.

☐

What personal data will it process, on what lawful basis, and is all of it necessary for the stated purpose?

Be specific about students, staff, parents, and any special category data. The principle of data minimisation (GDPR Art. 5) asks us to collect only what is necessary for the purpose we have defined.

☐

Have we completed the necessary data protection due diligence?

This should include confirming the lawful basis for processing, whether a Data Protection Impact Assessment (DPIA) is required, and reviewing the Data Processing Agreement (DPA) alongside the vendor's privacy policy and security documentation — including any international data transfers (e.g. Standard Contractual Clauses). As the data controller, the school remains responsible for determining whether the use of the tool is lawful and appropriate.

☐

Where is data stored, who can access it, and under what safeguards?

Consider hosting region, sub-processors, and vendor staff access, alongside the technical and organisational measures in place to protect the data.

☐

What security assurances does the vendor provide, and how do these align with our own expectations for risk, access, and incident response?

Look beyond storage to the wider security posture: certifications (e.g. ISO 27001, SOC 2), vulnerability management, breach notification commitments, and resilience expectations proportionate to how critical the system is to school operations.

☐

Have IT, the DPO, and senior leadership all reviewed it?

Cross-functional sign-off before adoption — not after a department has already started using it. This is the point at which institutional accountability is formally taken, drawing together everything the previous questions surfaced.

2

Additional considerations

Cross-cutting questions that apply across all stages, not only at adoption. Particularly relevant for AI-enabled tools and any system with potential to influence decisions about students or staff.


☐

What level of risk does this system represent in our context?

A proportionate, risk-based assessment — in line with the EU AI Act's tiered approach. The same tool can be low-risk in one setting and high-risk in another; what matters is how it is used here, with whom, and for what purpose.

☐

Where does human judgment remain central?

Be explicit about which decisions the system supports versus makes. Under the EU AI Act, some uses of AI in education may be high risk meaningful human oversight is essential.

☐

Is the system explainable to the people it affects?

If a parent or student asked why the system produced a particular output, could a member of staff give a coherent answer?

☐

Has the potential for bias or unfair outcomes been considered?

Models trained on partial or non-representative data can systematically disadvantage particular groups. Ask the vendor what testing has been done, and consider how outcomes will be monitored once the tool is in use.

☐

Is school data used to train the vendor's models?

Default settings vary by vendor and change over time. Confirm the current position in writing — and whether you can opt out.

3

During pilot

The picket fence. Setting the conditions under which the tool grows.


☐

Is the pilot time-limited, with defined success criteria?

"We'll see how it goes" tends to become permanent. Set the end date and the questions the pilot must answer before you start.

☐

Is it clear to staff which tool is approved for which purpose?

Shadow IT often grows where boundaries are unclear. Make the boundaries explicit so autonomy can sit comfortably alongside it.

☐

Does the use of this tool raise any safeguarding considerations?

Particularly for student-facing tools: content moderation, contact features, age-appropriateness, and how concerns would be raised and acted upon. Safeguarding is often the dimension most easily overlooked in vendor conversations.

☐

Have students, parents, and staff been informed appropriately?

Transparency is both a regulatory requirement and a trust signal. Quietly introducing a tool that affects the community rarely ages well.

☐

Is there a route for raising concerns?

A named owner, a known channel, and a willingness to act on what comes back through it.

4

Ongoing review

Cross-cutting questions that apply across all stages, not only at adoption. Particularly relevant for AI-enabled tools and any system with potential to influence decisions about students or staff.


☐

What level of risk does this system represent in our context?

A proportionate, risk-based assessment — in line with the EU AI Act's tiered approach. The same tool can be low-risk in one setting and high-risk in another; what matters is how it is used here, with whom, and for what purpose.

☐

Where does human judgment remain central?

Be explicit about which decisions the system supports versus makes. Under the EU AI Act, some uses of AI in education may be high risk meaningful human oversight is essential.

☐

Is the system explainable to the people it affects?

If a parent or student asked why the system produced a particular output, could a member of staff give a coherent answer?

☐

Has the potential for bias or unfair outcomes been considered?

Models trained on partial or non-representative data can systematically disadvantage particular groups. Ask the vendor what testing has been done, and consider how outcomes will be monitored once the tool is in use.

☐

Is school data used to train the vendor's models?

Default settings vary by vendor and change over time. Confirm the current position in writing — and whether you can opt out.

-  OpenApply
-  ManageBac+
-  Atlas
-  SchoolsBuddy
-  Vectare