

## Formulating Retention Policies for Education

### The Need for Electronic Records Retention Policies

Schools need to look at defining a formalized retention policy for electronic records and email documents. This policy should be based on the institution's retention needs from statutory and legal perspectives, as well as its own internal auditing requirements. In many cases, there may already be records retention policies in place, which should be modified to include electronic records.

When defining their retention policy, organizations should be aware of various driving factors:

#### Access to Information

As publicly funded organizations, most educational institutions are governed by the State's Access to Information legislation. Thus, in defining their electronic records policies, academic entities should check the retention time frames and the nature of the information that individual states mandate must be retained to meet open records request directives.

While schools may be subject to the state's access to information policy, it is critical that they develop their own policies for handling open records requests. They can use the state's policy as a guideline and elaborate on it, so that when they are faced with a records request, there is a clear procedure and policy for fulfilling it.

An academic organization's policy regarding open records requests should state the procedure for requesting this information, as well as specify the type of information the school will provide. Most Access to Information legislation makes the provision that not all information is accessible. The school should clarify those cases when information will not be released, for instance, if it is felt that by doing so would not be in the best interest of the school. There are also provisions in the legislation for an information access service fee for gathering and providing the information to the requestor. It is

important that schools understand these legislative requirements and provisions when they create their policies to deal with all requests for electronic discovery.

#### Legal Discovery

Electronic data is becoming the most prevalent source of evidence in most civil trials and organizations are finding themselves under great pressure and financial burden to produce electronic records in the course of litigation procedures. There are many legal opinions on which information or how much information to keep, but the consensus among legal experts dealing with electronic records is to save more information rather than less. This view is primarily based on the fact that email records by their very nature are difficult to destroy completely and so having more evidence in court is more beneficial than the other way around.

#### Internal Auditing

As with most educational institutions and especially K-12 organizations, the email correspondence between teachers and students, as well as teachers and parents, needs to be audited to ensure appropriate conduct and proper use of system resources. Most school email policies state that all email is subject to review, but few schools actually conduct regular reviews due to lack of the appropriate technology that would allow email audits and shortage of human resources to implement such controls.

It should be noted that while legal discovery and access to information requests could go back years, auditing of day-to-day communications typically comprises short-term monitoring.

## Save Everything or Save Some Things?

The majority of current legislation postulates, and legal advisors confirm it, that there is no reason to save all email messages and that transitory information and “junk” can and should be deleted from the system. The main problem arises in determining what should be kept and what constitutes transitory information that should be deleted. The second issue has to do with the risks of empowering users to make those decisions.

### Option 1: Save Some Things

This is the desired policy, but it has a catch. In order to implement it, the organization must develop a highly formalized data retention policy which outlines the individuals’ responsibility to retain information on behalf of the organization and also provides clear guidelines as to what information is acceptable to be destroyed and what information must be kept. In addition, the policy needs to state how the information must be kept. This policy has to be communicated to staff as part of an internal policy enforcement program. It also needs to be audited in order to ensure that it is being conformed to.

Unfortunately, practice shows that policy creation, education, and enforcement as the three aspects of data retention prove to be too much overhead for most organizations in terms of effort and resource allocation. Instead, most organizations opt for Option 2 – the “save everything” approach - as a preferred route.

### Option 2: Save Everything

This is the default policy when organizations are unable to define and/or enforce formal retention policies. In that scenario, the requirements are simply passed down to IT as a technical issue. The underlying premise to this approach is that adding storage is cheaper and faster than allocating resources for designing, implementing, enforcing, and monitoring a retention policy.

## Destruction Policies

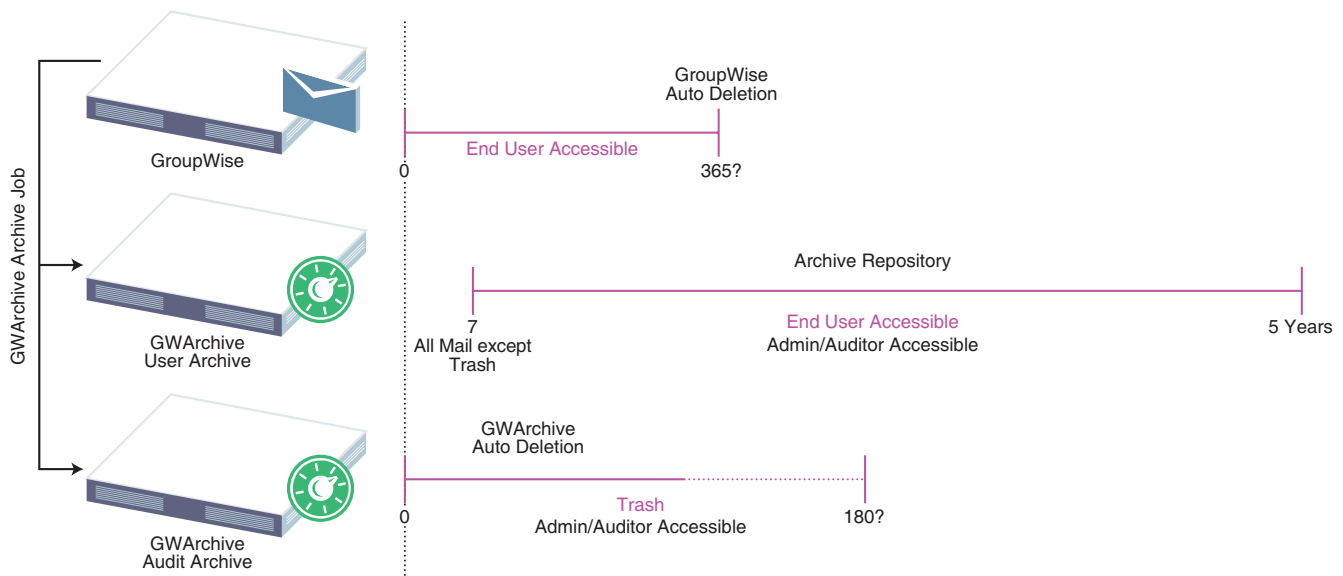
With any retention policy there is an associated destruction policy. This policy should not only apply to email in the live system and in the archives, but must also extend to all forms of electronic data, including backup tapes, personal archives, and even IMAP/POP clients which may have copies of email on the local workstations.

## Typical GWArchive Policy Scenarios for Educational Institutions

The typical retention policies created for the majority of educational organizations is one of 100% retention with separated trash. In this scenario, a GWArchive policy is configured to capture all email. The system allocates two separate repositories for the archived email: one for email messages in users’ inboxes and Cabinet folders, and one for the trash.

This scenario meets the following objectives:

1. 100% of the information is kept for a specified number of days that correlates with the organization’s backup tape destruction policy. This way in the event of an electronic discovery request, there is no need to restore backup tapes.
2. Trash can be subject to a different retention policy from that of the remaining email. If users are allowed to delete non-business-related/transient messages, the trash can be kept and audited separately.
3. Trash can either be shown or hidden from users when they access their personal archives. In the latter case, users are left with the illusion that email is not being kept, so there will be fewer requests to allow them to delete it.



The typical policy as illustrated introduces an overlap of information between the live and archive systems. This is necessary to balance 100% retention with the ability to purge trash from the system in a timely fashion and to ensure ease of searching of more current messages. Typically, there is a 7-day grace period, or “Action Delay”, prior to items being captured and placed into the archive. This approach to retention provides users with a one-week window within which to action a message item by opening it, deleting it, or moving it into a specific folder. It is important to configure the action delay period in such a way as to provide a balance between retained trash and users’ processing of messages, since at the point of capture the system takes a snapshot of the mailbox and includes all message properties and message locations to incorporate to add into the archive repository.

With some education institutions such as K12, there may be times, such as spring break, Christmas, and summer vacation when users may not access their mailboxes at all. During these times, the 7-day cycle may or may not be appropriate. In these instances, the solution is to simply suspend message processing during this time or create specific policies to be run during holidays which dictate a higher action delay threshold.

### In Conclusion

Implementing formal archiving policies for email will simplify the process of records retention and provide a single point of access and knowledge. If there are legal discovery or public access requests, schools can be certain as to what information is available to them and where that information exists, thus reducing costs and providing quicker discovery turn-around.

Without formal policies endorsed by upper management, most IT initiated policies quickly become diluted through the introduction of “exceptions” due to user “pushback” which threaten to compromise or undermine the retention mandate.

What to keep and for how long to keep it are typically standard from school to school and state to state, but the methods of how that information is captured and retained is largely left to the organization. Important considerations in this context are the level of automation that the retention solution provides, as well as to what degree it ought to be managed by the respective school’s faculty and administrative staff.

