Data Loss Prevention

Within the Office 365 Security & Compliance Center, you can set data loss prevention (DLP) policies. These policies can identify, monitor and automatically protect sensitive information across Office 365.

With a DLP policy you can:

Identify
Sensitive, personal information such as credit card or passport numbers can be identified when stored across multiple locations, including emails or on your OneDrive.

Prevent
Users can be blocked from accessing certain data via user assigned tags. Policies can also be set to prevent information being shared.

Alert
Users will be warned if they are about to send sensitive information to a user who does not have permission to view the data. This will be via an alert email or notification in Outlook.

Report
Once your DLP policies are in place, you'll want to ensure they're working effectively. With DLP reports, you can view the number of DLP policy and rule matches over time. For each report, you can filter those matches by location, time frame, and even narrow it down to a specific policy, rule, or action.

How DLP policies work
DLP detects sensitive information by using deep content analysis (not just a simple text scan). This deep content analysis uses keyword matches, dictionary matches, the evaluation of regular expressions, internal functions, and other methods to detect content that matches your DLP policies.

DLP policies are made of conditions and actions:
Condition = the content must match before the policy is enforced.
Actions = the policy you want to automatically enforce one the condition is met.