Data Sharing and Confidentiality Requirements

Compliance with New York State Education Law Section 2-d

This Agreement is made by and between the Akron Central School District (the "District") and __PaperCut Software Pty Ltd (the "Company"), collectively referred to herein as the "Parties." The District is an educational agency, as that term is defined in Section 2-d of the New York State Education Law ("Section 2-d"), and the Company is a third party contractor, as that term is defined in Section 2-d. The District intends to enter into this Agreement by which the Company shall have access to Student Data and/or Teacher or Principal Data regulated by Section 2-d for purposes of _PaperCut Software's printer and multi-function device management software and related services.

The Company agrees to comply with the following provisions as set forth in Section 2-d prior to the District's signing of contracts and shall submit to the District a copy of its Data Security and Privacy Plan as well as the completed attached Addendum for review before final approval of this Agreement and should stay in effect for the duration of this Agreement.

A. The release by an "Educational Agency" of certain Student Data and/or Teacher or Principal Data to a "Third Party Contractor" is subject to the requirements of Section 2-d; and

B. Upon which time the Company receives, holds, or has access to Student Data and/or Teacher or Principal Data originating from the District that uses the Company's product/service pursuant to the newly-signed Agreement, the Company agrees to conform to the requirements of Section 2-d;

C. Additionally, based upon the mutual covenants and understandings between the Parties, the Parties hereby agree to the following definitions with respect to shared Student Data and/or Teacher or Principal Data, as applicable:

1. "Student Data" means personally identifiable information from student records that the Company receives or has access to from the District. "Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 C.F.R. §99.3 implementing the Family Educational Rights and Privacy Act ("FERPA"), at 20 U.S.C. 1232g.

2. "Teacher or Principal Data" means personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under New York State Education Law Section 3012-c.

3. "Third Party Contractor" means any person or entity, other than an educational agency, that receives Student Data and/or Teacher or Principal Data from an

educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

4. "Educational Agency" means a school district, board of cooperative educational services, school, or the New York State Education Department.

5. "Parent" means a parent, legal guardian, or person in parental relation to a student.

6. "Student" means any person attending or seeking to enroll in an educational agency.

7. "Eligible Student" means a student eighteen years or older.

8. "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, NY 12234.

1. 9. "Unauthorized Disclosure" or "Unauthorized Release" means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

D. Student Data and/or Teacher or Principal Data that the Company receives or has access to, including by any of its subcontractors or assignees, shall not be sold, used or disclosed for any marketing or commercial purposes.

E. The Company shall maintain the confidentiality of the Student Data and/or Teacher or Principal Data to which it has access in accordance with state and federal law and the District's data security and privacy policy.

F. The exclusive purposes for which the Company may receive or have access to Student Data and/or Teacher or Principal Data is delineated in the Underlying Contract. The Company agrees to not use the Student Data and/or Teacher or Principal Data for any other purposes.

G. The Company further agrees that it will protect the confidentiality, privacy and security of Student Data and/or Teacher or Principal Data in accordance with the District's Parents Bill of Rights for Data Privacy and Security ("Bill of Rights"). A copy of the Bill of Rights is attached hereto as **Appendix A.**

H. The Company agrees that any of its officers or employees, and any officers or employees of any subcontractor or assignee of the Company, who may be granted access to the Student Data and/or Teacher or Principal Data, have received or will receive training on

the federal and state law governing confidentiality of such data prior to receiving the data or access to the data.

I. The Company acknowledges that as a "Third Party Contractor" of the District, it has certain statutory and regulatory obligations under Section 2-d with respect to Student Data and/or Teacher or Principal Data, and agrees that failure to fulfill one or more of these statutory and/or regulatory obligations shall be deemed a breach of both the Underlying Contract and this Agreement:

1. To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;

2. To comply with the District's data security and privacy policy; Section 2-d and its corresponding regulations;

3. To limit internal access to education records and shared Student Data and/or Teacher or Principal Data to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA) (*i.e.,* the individual needs access to the Student Data and/or Teacher or Principal Data in order to provide the contracted services);

4. To not use student education records or shared Student Data and/or Teacher or Principal Data for any purpose not explicitly authorized in this Agreement or Underlying Contract;

5. To not disclose any personally identifiable information to any other party who is not an authorized representative of the Company using the information to carry out the Company's obligations under the Underlying Contract, unless:

   a. the parent or eligible student has provided prior written consent; or

   b. the disclosure is required by statute or court order, and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

6. To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody; and

7. To use encryption technology to protect personally identifiable information while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

J. The Company further acknowledges the following additional obligations under Section 2-d regarding breach and unauthorized release of Student Data and/or Teacher or Principal

Data, and agrees that failure to fulfill one or more of these additional statutory obligations shall be deemed a breach of both the Underlying Contract and this Agreement:

1. To promptly notify the District of any breach of security resulting in an unauthorized release of personally identifiable data by the Company or its subcontractors or assignees in violation of applicable state or federal law, the District's Parents Bill of Rights set forth in **Appendix A** of this Agreement, or obligations relating to data privacy and security contained within this Agreement, in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after the discovery of such breach.

2. The Company must cooperate with the District and law enforcement to protect the integrity of investigations into the break or unauthorized release of personally identifiable information.

3. In the event that the District is required under Section 2-d to notify affected parent(s), student(s), eligible student(s), teacher(s) and/or principal(s) of an unauthorized release of Student Data and/or Teacher or Principal Data by the Company or its assignees or subcontractors, the Company shall promptly reimburse the District for the full cost of such notification.

K. The Company will ensure that any subcontractors or assignees with whom it shares Student Data and/or Teacher or Principal Data will abide by the data protection and security requirements of Section 2-d, by requiring them to execute written agreements which subject them to the terms of this Agreement.

L. Upon expiration of this Agreement without a successor Agreement in place, the Company shall assist the District in exporting all Student Data and/or Teacher or Principal Data previously received by the Company, if any, back to the District. The Company shall thereafter securely delete any and all data remaining in the Company's possession or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all data maintained on behalf of the Company in secure data center facilities within ten (10) days of termination of services, and provide confirmation of same to the District. The Company shall ensure that no copy, summary or extract of the data or any related work papers are retained on any storage medium whatsoever by the Company, its subcontractors or assignees, or the aforementioned secure data center facilities. To the extent that the Company and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, the Company and/or its subcontractors or assignees will provide a certification to the District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

M. In the event that a parent, student, eligible student, teacher or principal wishes to challenge the accuracy of the data concerning that student, eligible student, teacher or principal that was shared with the Company and is maintained by or under the control of

the Company, that challenge shall be processed through the procedures provided by the student's school district of residence for amendment of education records under FERPA. The Company will be notified by the District of the outcome of any such challenges and will promptly correct any inaccurate data it or its subcontractors or assignees maintain.

N. Student Data and/or Teacher or Principal Data transferred to the Company by the District will be stored in electronic format on systems maintained by or under the direct control of the Company in a secure data center facility, or a data facility maintained by a New York board of cooperative educational services, within the United States. The measures that the Company will take to protect the privacy and security of the Student Data and/or Teacher or Principal Data while it is stored in this manner shall be those associated with industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

O. The Company hereby acknowledges that it may be subjected to civil penalties for failure to property protect and secure student, teacher or principal data, as outlines in Section 2-d.

P. To the extent that any term of the Underlying Contract conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect. In the event that the Company has Terms of Service (TOS) that may otherwise be applicable to its customers or users of its product/service, to the extent that any term of such TOS conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Q. Any revisions to this Agreement shall be by mutual written agreement of the Parties. Notwithstanding the foregoing, the Parties acknowledge that modifications to this Agreement may be necessary in the future to ensure compliance with Section 2-d and its applicable regulations, issuance of further guidance by the New York State Education Department, and the District's Policy on data security and privacy subsequent to the Parties' execution of this Agreement. Necessary modifications at that time will include incorporation into this Agreement of the Company's data security and privacy plan that will outline how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the District's Policy on data security and privacy. The Parties agree to act in good faith to take such additional steps as may be necessary at that time.

APPENDIX A

AKRON – Parents' Bill of Rights for Data Privacy and Security

The NYS Education Department's
Education Law §2-d Bill of Rights for Data Privacy and Security

Parents and eligible students[1] can expect the following:

1. A student's personally identifiable information (PII)[2] cannot be sold or released for any commercial purpose.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.

3. State and federal laws,[3] such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of a student's PII, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by NYSED is available for public review at www.nysed.gov/data-privacy-security, and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be submitted to NYSED online at www.nysed.gov/data-privacy-security, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, by email to privacy@nysed.gov, or by telephone at 518-474-0937.

6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

---

[1] "Parent" means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. "Eligible Student" means a student 18 years and older.
[2] "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter.
[3] Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data.

ADDENDUM – SUPPLEMENTAL INFORMATION

The supplemental information obtained below will be included with the Akron Central School District's (the "District") Parents' Bill of Rights as required by New York State Education Law Section 2-d [3][c]. The Parents' Bill of Rights and this supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

1. The Company agrees to use Student Data and/or Teacher or Principal Data for the exclusive purposes listed below:

The provision and support of PaperCut Software's printer and multi-function device management software and related services.

2. The Company will provide to the District, in writing, a statement indicating how it will ensure that any subcontractors, or other authorized persons or entities to whom the Company will disclose such Student Data and/or Teacher or Principal Data, if any, will abide by data protection and security requirements, including, but not limited to, those outlined in applicable state and federal laws and regulations (e.g., FERPA, Education Law Section 2-d):

1. Only allowing for the transfer of data to the extent such transfer is strictly necessary for the exclusive purpose (which, in most cases, means that no personal or sensitive data will be transferred at all 2. Ensuring that any subcontractors handing personal or sensitive data are contractually obliged to keep the data safe on terms which re consistent with our obligations under this plan.

3. The Company will provide the District with a written description of what will happen to Student Data and/or Teacher or Principal Data upon expiration of this Agreement or other written agreement (e.g., whether, when, and in what format data will be returned to the District, and/or whether, when, and how the data will be destroyed).

When the contract expires, protected data will, upon the written request of the District, be deleted by the Company, and may be exported for use by the District before being deleted.

4. The Company will provide the District with a written description of how a parent, student, eligible student, teacher or principal may challenge the accuracy of the Student Data and/or Teacher or Principal Data that is collected.

In the event that a parent, student, eligible student, teacher or principal wishes to challenge the accuracy of the data concerning that student, eligible student, teacher or principal that was shared with the Company and is maintained by or under the control of the Company, that challenge shall be processed through the procedures provided by the student's school district of residence for amendment of education records under FERPA. The Company will be notified by the District of the outcome of any such challenges and will promptly correct any inaccurate data it or its subcontractors or assignees maintain.

5. The Company will provide the District with a written description of where the Student Data and/or Teacher or Principal Data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure that such data will be protected, including, how such data will be protected using encryption while in motion and at rest.

The measures that the Company takes to protect the Student Data and /or Teacher or Principal Data will align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, which includes our NIST framework response.

BY THE DISTRICT:

X [redacted]

Andrea Kersten
Superintendent

11/14/2024

Date

BY THE VENDOR:

X [redacted]

James Fergusson

Head of Global Finance

Date: 15 October 2024

A lot of companies publish intimidating, detailed "legal speak" privacy policies

At PaperCut, we've decided that our privacy policy should be simple and easy to understand. The PaperCut Privacy Policy sets out how we handle personal information, and applies across our whole business and all our products and services. Before we get into what this actually means for you, we do need to get some of the basic legal stuff out of the way.

- If you access our site and/or use our products and services, you consent to the terms of the PaperCut Privacy Policy and agree to be bound by it and our EULA and/or Terms of Service (based on the product you're using).
- Getting back to the PaperCut Privacy Policy, we're a customer-focused company and that means we genuinely care about your privacy. We'll treat your personal information the way we'd like others to treat ours.
- Feel free to check out our PaperCut MF and NG EULA, the PaperCut Pocket and PaperCut Hive Terms of Service, the PaperCut Views Terms of Service, or the Print Logger EULA alongside this policy.

Definitions

- Before we begin, let's make sure we're all on the same page about who's who. We're PaperCut Software Pty Ltd (ACN 650 500 413). When we say 'us', 'we', 'our' or 'PaperCut', we're referring to ourselves.
- When we mention "you" or "your", we're referring to people who use or engage with the PaperCut brand, products and services such as PaperCut MF™, PaperCut NG™, PaperCut Hive™ and PaperCut Pocket™. It also refers to people visiting our sites, including engaging in social media.
- Trusted Partners – Authorized Partners, Resellers, and Manufacturers.

What type of information do we collect?

PERSONAL INFORMATION

- Personal information that identifies you as an individual or relates to an identifiable individual such as your name, title, company name, job function, postal address, telephone number, username,or email address.

- If you submit any personal information relating to other people to us or to our Trusted Partners in connection with your workplace, you agree that you have the authority to do so and permit us to use the information in accordance with the PaperCut Privacy Policy.
- In order to be able to provide PaperCut products or services, there will be times when we'll obtain information about you from other people such as our Trusted Partners.
- Your IP address number that is automatically assigned to the computer that you're using by your Internet Service Provider (ISP). An IP address may be identified and logged automatically in our server log files whenever you access the PaperCut sites, along with the time of the visit and the page(s) that you visited.
- At times, you may disclose personal information from publicly available sites (i.e. from social media, blogs, websites and other services) where you're able to post information and materials. Please remember that this information is publically available.
- We may also collect personal information from job applications to assess an applicant's suitability for employment.

OTHER INFORMATION

- Other information is any information that does not reveal your specific identity or does not directly relate to an identifiable individual. This might include URLs of pages you visit and the device, operating system, and browser you use and the time of your visit. We collect this information to help us understand how our websites are working and how we could improve them/our services.
- We use anonymous aggregated data provided by you and other users of the PaperCut products for the purpose of best practice, benchmarking, forecasting, and education.
- At times, we publish aggregated information. However, please feel safe in knowing that we won't publish information that identifies you without your prior approval.
- We do retain messages you post to our website or blog.
- If you download a PaperCut Software trial and you enter your contact details but you do not proceed with license purchase, we may contact you.

We have different ways of collecting information

PERSONAL INFORMATION

- If you're using our website, we may collect information directly from you when you download our free trial, register for events (including webinars), contact us, subscribe

to our email newsletters, download content, register to use our sites (e.g. the PaperCut Portal), or job applications.

- You or a Trusted Partner may supply us with test data, database backup, or system logs to help us find and address bugs. This data may include personal information such as usernames.
- We may collect personal information from you if you attend one of our events, or an event that we're attending, or during calls with sales and support teams, or when you contact us.
- Our software applications will never secretly prompt you to install some gee-wiz browser toolbar. As software geeks, we needed to put that one in the list.
- If you use one of our web-based services, components of those services may collect personal information in order to provide you with that service.
- In relation to the "scan to cloud" feature of certain PaperCut software (which enables users to scan documents to Google, DropBox etc), we store scanned files in an encrypted format for up to 24 hours, after which time they are deleted. However, we retain summary information relating to scan jobs that may include personal information such as usernames.
- In order to enhance our ability to provide relevant marketing, offers, and services to you, we may obtain information about you from other sources, such as public databases, our Trusted Partners, social media platforms, and from other third parties.

OTHER INFORMATION

Certain information is collected by most browsers or automatically through your device, such as your computer address, computer type, screen resolution, operating system name and version, device manufacturer and model, language, Internet browser type and version, and the name and version of the sites you're using.

HERE'S HOW WE USE COOKIES AND ANALYTICS

- The type of cookies we're talking about are web beacons and similar technologies that record log data. They're small text files stored on your computer for record-keeping purposes, every time you visit our website.
- We love analysing data (it's our inner geek) so we collect anonymous data, too. While it doesn't directly identify you personally or contain any other information about you, it does identify your computer.
- We and our third-party service providers may use a combination of "persistent cookies" (cookies that stick around until you or your browser deletes them or they

expire) and "session ID cookies" (cookies that are deleted when you close your browser) on the website.

- From a website point of view, the cookie helps us track overall site usage, and track and report on your use and interaction with ad impressions and ad services. We use this kind of information to improve the functionality and experience of PaperCut Products, Services and our website.
- We use web analytics services (currently Google Analytics).
- The other type of information we collect is non-identifiable data to help us derive global or industry usage metrics to assist forecasting, benchmarking, and trend analysis. We use it to help us crunch the numbers in the background.
- For PaperCut NG and PaperCut MF, we collect Feature Usage Data to help us improve our products. It's handy for us to understand how our product is being used so we know which features to invest time into future development. To turn off the collection of Feature Usage Data, simply navigate to Options >> Advanced options >> System Usage Data and disable Send system usage data.
- We don't store credit card details, nor do we process credit cards ourselves. Instead we only use trusted sources. All direct payment gateways adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, MasterCard, American Express, and Discover.

How we use this information

Overall, the key reason for us collecting personal information is so we can provide our customers with better support and to improve their user experience. But also to:

- Understand and improve our products.
- Assist you with technical support issues or other issues relating to our Products and Services. This may include sharing your support requests and data logs with our Trusted Partners (for example Authorized Solution Centers).
- Send you operational information (information required for us to continue providing your product and/or service i.e. advising your Maintenance & Support is about to expire).
- Communicate with you and respond to your inquiries and fulfil your requests (such as sending you requested materials) as well as information and materials regarding our products and services.
- Send email and/or SMS marketing communications e.g. newsletters and product upgrades. These will only be sent to you if you have requested the information or

opted in to receiving marketing communications. We'll provide you with instructions for how you can remove yourself from that mailing list if you so wish.

- Record your marketing and communication preferences so we can keep you informed about our product updates and service offerings.
- Provide you with usage reports.
- Perform our general business purposes (such as finance reporting and identifying usage trends campaign effectiveness).
- Anonymously aggregate your data provided with other users of PaperCut products for the purpose of best practice, benchmarking, forecasting, and education.
- Process a job application you've submitted and communicate with you.
- Successfully manage "scan to cloud" services (we use scan job summary information to provide users with reports or auditing on their use of the service).

TWO MORE THINGS TO NOTE

- We'll keep your personal information for no longer than is necessary to fulfil the purposes for which it was collected.
- Where we have granted you a perpetual licence we may not be aware that you have ceased using our product, so we'll keep your data until you notify us that you no longer use our software.

For our Authorized Partners and Resellers

- A prerequisite when becoming an Authorized Partner or Reseller is to provide your contact details (email and mobile) to enable PaperCut to provide operational notifications and communications. For example, your customer's Maintenance & Support is about to expire, and product release updates.
- We'll email you newsletters and other marketing communications only if you have opted in, and we'll provide you with instructions as to how you can remove yourself from that mailing list if you so wish.

Sharing of your data

- PaperCut has Trusted Partners that sell and implement PaperCut products and services. At times, we'll need to disclose personal information to our Trusted Partners for the purposes described above.
- We may contract other companies and people to perform tasks on our behalf and may at times need to share your personal information with them to provide products or services to you, or to otherwise communicate with you. Examples may include removing repetitive information from customer lists, analyzing data, conducting

billing, engaging technical support for our services, providing customer service, and performing analysis related to our products or services.

- At times, prospective customers contact us directly that need to be referred to an Authorized Partner due to the suitable product not being sold directly by us. In these instances, we ask for your permission to pass your details to our Trusted Partner.
- We use service providers, like those who provide us with cloud storage solutions, to provide the best service to our customers. Some are based outside Australia (in places like Europe, UK, Asia and the US). To the extent information received by Google APIs is used by the Scans for PaperCut app (Scan to Google Drive and Scan to Shared Google Drive) or transferred to another app by Scans for PaperCut, that use and transfer will adhere to the Google API Services User Data Policy, including the Limited Use Requirements.
- We'll also disclose your personal information if we are required by law or as permitted by the applicable laws.

The security of your information is our top priority

- We store personal information on secure servers that are managed by us and our service providers, and occasionally hard copy files that are kept in a secure location. Personal information that we store is subject to security and access controls, including username and password authentication and data encryption where appropriate.
- While we do take reasonable steps to secure your personal information from loss, misuse, interference and unauthorized access, modification and disclosure, you should be aware no security procedures or protocols are ever guaranteed to be 100 percent secure from intrusion or hacking, and there is therefore always some risk assumed by sharing personal information online.
- If there's a high risk of harm in the event of a breach, we'll report to our data protection authority as soon as possible after becoming aware of the breach and to the data subjects as soon as possible.

Your rights

- You can contact us at privacy@papercut.com to access, correct, or request deletion of any of your personal information that we store.
- Where you have provided your consent for us to use your personal information, you may withdraw that consent at any time. Please note that withdrawal of consent may prevent us from being able to provide products or services to you.

- To view or change the marketing material you receive, you can manage your data preference settings via the 'manage your preferences' link found at the bottom of any marketing communications you've received.
- You have the right to lodge a privacy complaint with a relevant supervisory authority. In Australia, the Privacy Commissioner's website is at www.oaic.gov.au.

Changes to these terms

We're always looking to improve PaperCut products and services and to provide you with new and exciting features. This means we may need to change our PaperCut Privacy Policy from time to time (i.e. our lawyers will tell us to change them...). But don't worry - we'll try to keep you informed when something is different.