We protect our resources

Protecting Newcrest and Third Party Property

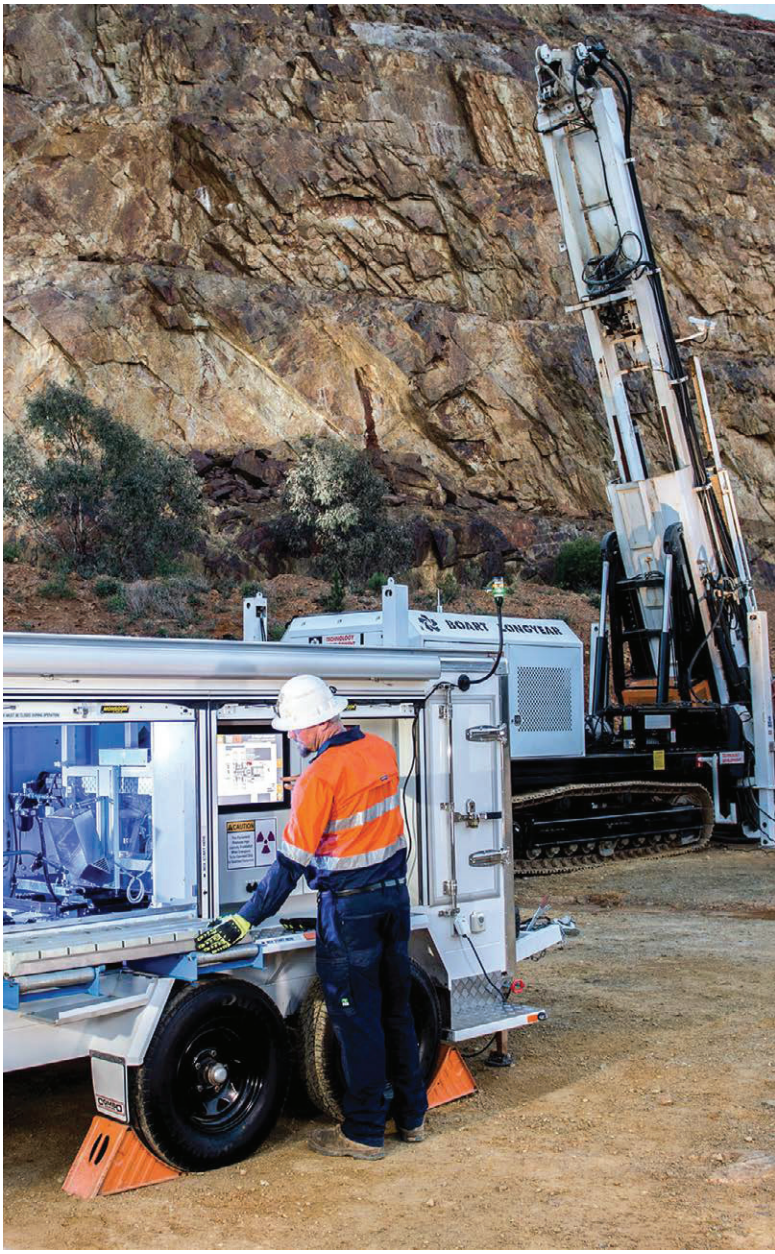
We are committed to protecting Newcrest confidential information and property at all times and making sure that we only use it for the benefit of the company.

Newcrest property includes physical property such as facilities, equipment, vehicles, computers and information technology systems. It also includes financial assets such as money and non-physical property such as intellectual property and confidential information.

Intellectual property includes patentable inventions, registered designs, copyright works and trademarks. Confidential information includes commercially sensitive information, business information and data, trade secrets, confidential operating procedures and know-how. Intellectual property and confidential information are found across our business. It's in operational processes, specifications, plans, drawings, financial data, equipment, software, branding and written documentation.

Intellectual property and confidential information are strategic and valuable assets. Their value can be lost if not managed correctly. Risks include sharing or using it in the wrong way, incorrect contractual wording and a failure to seek proper safeguards.

We are committed to complying with applicable laws in relation to intellectual property. We also respect the intellectual property rights and confidential information of third parties. Using intellectual property and confidential information of third parties in the wrong way can result in disputes. It can also damage Newcrest's reputation.



Our expectations of our people

Everyone at Newcrest must protect Newcrest property against damage, loss, theft or unauthorised access. It is expected that you:

- Only use Newcrest property when it's required by our work and to benefit the Company.
- Always follow our policies and procedures.
- Do not change, destroy, throw away or take Newcrest property without the right approval.
- Do not share Newcrest's intellectual property or confidential information without the right approval.
- Set up confidentiality agreements or make sure that third parties have agreed to confidentiality in writing before you share intellectual property and confidential information.
- Return all Newcrest property at the end of your employment.

It is also expected that you respect the intellectual property and confidential information of third parties such as our suppliers and competitors. Only use and share the intellectual property and confidential information of third parties as allowed by confidentiality agreements and third-party licensing terms.

If you're unsure, talk to your line manager or the Legal Team. Tell your line manager or consult with Legal if you:

- Suspect fraud, theft or wrongful use of Newcrest property.
- Suspect or become aware of the wrongful use of third-party intellectual property or confidential information.
- Think intellectual property could or has been created out of a project or work with third parties. Legal can make sure that Newcrest has the right contract terms and other safeguards in place.

Learn more

- Intellectual Property Strategy
- Information Technology and Data Management Policy

Who to contact for help

Your line manager

Legal Team

In practice

Scenario	Response
At work I invented a device that's helping our team to be more efficient. I think it could also help other companies. **Who owns this intellectual property?**	As set out in your employment contract, all intellectual property created while you are working for Newcrest belongs to Newcrest. This means that you cannot use it for non-Newcrest purposes without first obtaining permission to do so from Newcrest.
I'm finishing up my work at Newcrest. There are a few things from my work that I'd like to keep. **What can I keep and what must I leave at Newcrest?**	When you finish up at Newcrest, you must return all Newcrest property. This includes returning books, access cards, notebooks, software, computers, credit cards, keys, mobile phones, security passes and vehicles. You also need to return documents that include confidential information or relate to the business of Newcrest or any customer or supplier of Newcrest.

We do

Set up confidentiality agreements with third parties before starting negotiations or sharing Newcrest's intellectual property or confidential information.

Respect intellectual property and confidential information of third-parties by complying with third-party confidentiality agreements and licence terms.

Only use Newcrest property when required for your work and for Newcrest's benefit.

We don't

Misuse Newcrest property for our own private benefit.

Change, destroy, throw away or take Newcrest property without the right approval.

Share Newcrest's intellectual property and confidential information without the right approval and a confidentiality agreement in place.

Let third parties use Newcrest's trademarks and logos without the right approval.

Asset and Technology Management

Assets include physical and non-physical property, such as equipment, inventory, technology, intellectual property, company information and data.

We take care of our assets by doing the right operational, technical and maintenance work at the right time. Asset and Technology management also includes using the right plant and equipment, tools, parts, skilled workforce, applications, networks and systems as set out in our standards, so we work safely and maximise value.

We protect our assets throughout their lifecycle, from design through to disposal and strive to optimise their reliability across the production value chain. Robust information security is a primary consideration when designing, implementing, and using our assets and technology.

This approach helps us to meet our safety, environmental, operational, and financial goals and reduce risks and costs.

Our expectations of our people

We all have an obligation to safeguard our assets and to use them appropriately. We never knowingly misuse or cause damage to our assets.

Our responsibility to safeguard our assets also includes preventing and detecting fraud.

Learn more

- Asset Management Diagnostic Guideline
- Asset Management Standard
- Information Technology and Data Management Policy
- Keeping Important Company Information Confidential Guideline
- Security Policy
- Information Technology Usage Acceptance Form

Who to contact for help

Your line manager

Site IT Superintendent

Cybersecurity Advisor

Group Manager, Security

In practice

Scenario	Response
There's software that I want to help me do my work. **Can I download and install the software onto my Newcrest device?**	No. Only authorised and approved software is allowed on your Newcrest device. Installing unapproved software could put your device at risk of viruses or other malicious cyber vulnerabilities. If you require other software, ask the IT Service Desk. Remember, it is your job to keep your Newcrest provided devices safe.
My manager has a personal business. He uses Newcrest's assets for his business including Newcrest meeting rooms to meet with his customers and sends personal parcels on Newcrest's courier account. He also asks me to do small tasks for his business during work time. **Is this acceptable? What should I do?**	Newcrest's assets should only be used for Newcrest work. You shouldn't do or be asked to do work for an unrelated business during Newcrest work time. Using Newcrest assets for a non-Newcrest matter may amount to theft/fraud. Seek guidance from your local People Team, Ethics & Compliance Champion or report via the Speak Out channels.

We do

- Use Newcrest assets for company purposes only.
- Report any theft, misuse, loss, or fraud of our assets. We report the loss (such as a lost laptop) or theft of Newcrest information to our line manager immediately.
- Keep devices containing information that relates to Newcrest in a secure location.
- Use work resources in the way that they're intended to be used.

We don't

- Use Newcrest assets for personal gain.
- Permit unauthorised access to Newcrest sites or offices or access to our data or information technology.
- Share sensitive data without approval.
- Try to access sensitive data within applications without approval to do so.

Cybersecurity, Information and Data Protection

We're committed to protecting Newcrest business information and data by applying the right level of controls and educating our people on cybersecurity.

We're always improving our cybersecurity capability across Newcrest to prevent viruses, cyber-attacks, theft of our data and damage to our reputation.

Our systems, assets and data are the property of the Company. This includes Newcrest data stored both on your Newcrest devices and your personal devices.

Our expectations of our people

Everyone is responsible for keeping our systems and data safe. Whether you're an employee, business partner or contractor, we all must play our part. So when you use Newcrest's information technology and operational technology, always follow our company policies, standards, procedures and guidelines.

Here's how you can help keep our systems and data safe:

- Don't share your Newcrest passwords with anyone, especially people outside the Company. Don't write or store your password in a way that could be worked out by others.
- If you send our business data to third parties, you need to ensure you conform to the Information Technology and Data Management Policy. Depending on the type of data, you may need the approval of your line manager first. We don't share business data with others when there isn't a valid business or legal need.
- Don't forward emails from your business email address to your personal email address. This is to keep our data confidential as external email providers and personal devices are outside our safeguards. The Information Technology and Data Management Policy sets this out.
- Your Newcrest email address should only be used for work and never be used for personal purposes. So don't use your Newcrest email address when signing up to websites such as career or social media sites.
- Use applications recommended in the Application Usage Standard to safely and securely store documents. Never save Newcrest documents on your PC hard drive, external storage device or other locations such as Dropbox that aren't secure or backed up. Don't copy or transfer files that break any copyright laws.
- Use Newcrest-owned devices and software in the way they're intended. Safeguards have been set-up, so don't remove Newcrest mobile applications or device management software from your company phone or tablet. If you get a security notification or message, don't ignore it. Company assets or employees could be at risk.
- Unsecured networks are unsafe. Don't connect Newcrest devices to them.

If you're unsure about how to use our systems or devices, ask your line manager or Newcrest Information Technology for training. Ask the IT Service Desk if you need software or information technology services from a supplier or third party.

Learn more

- Security Policy
- Information Technology and Data Management Policy
- Information Technology Usage Acceptance Form
- Keeping Important Company Information Confidential Guideline
- Social Media Standard
- IT and Platforms Portal

Who to contact for help

Your line manager

Site IT/OT Superintendents

Manager Infrastructure and Cybersecurity

In practice

Scenario	Response
I think I've received a phishing email? **What should I do?**	Click on the Report Suspicious button on your Outlook client menu bar. Do this either on your laptop or mobile device. You must also contact the IT Service Desk if you've accidentally clicked on a link that looks suspicious.
I want to share information and data with a supplier. **What's the best way to do this securely?**	First, always check and verify the identity of the third party when asked for information. If the request is not expected or unusual, ring or text them, rather than using email, to confirm that the request is legitimate. Second, use a secure and protected method to share data. Refer to the Application Usage Standard and guidelines on options to share data securely.

We do

Question all requests for access to confidential information or login user names or passwords from people inside and outside the Company.

Ensure that our Newcrest devices are up to date with security updates and fixes provided by Newcrest. This is so that they don't create security problems for our systems.

Lock our screens when leaving them unattended.

Protect and maintain the confidentiality of information about our business, plus details about our people and stakeholders.

Register for Mandatory Multi Factor Authentication to provide extra protection for our systems.

We don't

Download or copy illegal content from the internet or storage devices onto Newcrest devices. Examples include pornography or anything of a sexual, sexist, derogatory or discriminatory nature.

Illegal downloads can also expose us to cyber-attacks.

Install unapproved apps or systems onto Newcrest devices.

Provide information that isn't public to any person or company without the proper approval.

Open attachments or click on links in emails that come from senders who we don't know or are in emails that we don't expect.

Use any storage solutions that haven't been approved such as hard drives, USB's, personal emails or personal cloud environments to send, receive or store Newcrest data.

Re-use passwords that we've used before. Make sure the passwords that we use for work aren't also used for other websites.

Accuracy in Company Records

Using and handling information in an accurate way is critical to our integrity and reputation. It's especially important that our company records are accurate.

Each of us create company records when we send emails, write memos, reports and presentations. Company records include financial and non-financial information and accounts. We all have a part to play in keeping accurate company records. This is so that Newcrest continues to meet its obligation to keep the market fully informed about our activities. Our stakeholders rely on us to be open and honest.

Our expectations of our people

You must make sure that the information you record or report is honest, accurate, timely and transparent. It's important that the records you create don't give a false view of the state of our business. Whether you're writing a negative or a positive report, you need to bring the same clarity and honesty.

Our values – integrity and honesty, caring about people, high performance, working together, innovation and problem solving – guide how we communicate and record information.

We also provide you with standards and policies to help you. We must follow these internal standards as well as financial, legal and regulatory requirements.

If you see or suspect something, or a report doesn't seem right, then please speak up.

Learn more

- Document Management Standard
- Market Releases and Investor Relations Policy
- Media and External Communications Policy

Who to contact for help

Your line manager

Ethics & Compliance Champions

Company or Deputy Secretary

In practice

Scenario	Response
My team are capable and trustworthy. **Is it ok to assume the information they prepare for external release is accurate when I sign it off?**	You must check the information and ask questions to make sure of your understanding. You need to satisfy yourself that the information is reliable before signing it off.
I help my team process invoices and expenses. **What evidence do I need to check and keep to support these financial transactions?**	When you put through a financial transaction, you need to check that the source documents, such as invoices or receipts, are accurate and complete. You must also save source and supporting documents in Newcrest's systems.

We do

Keep accurate, complete and true company records in line with relevant laws, regulations, policies, standards and procedures.

Follow company standards and procedures to make sure all transactions are properly approved and accurately recorded.

Cooperate fully, openly and honestly with internal and external auditors, relevant authorities and regulators.

We don't

Encourage or allow others to do something that would harm the accuracy or integrity of company records.

Conceal, change or fake records or lie about any facts or situations in company records for personal gain or for other reasons. For example, changing records to try to get a bonus, a pay rise, a promotion or commission.

Destroy company records unless we're confident it's ok to do so.

External Communications

We communicate with media and other external stakeholders in a timely, fair and consistent way.

As a publicly listed company, we follow laws about how we disclose information so that investors can make informed decisions.

Our expectations of our people

Sometimes you may know confidential or sensitive information as part of your work, which must not be shared unless you're authorised to do so.

You may have the opportunity to present at or be on a panel discussion at an external conference. Before accepting, you should ask yourself whether the event relates to your job, if there's a clear benefit for Newcrest and importantly get approval from the Head of Group Communications.

Speak to your line manager or Group Communications if you're unsure about:

- how to engage with external stakeholders; or
- what can be shared outside Newcrest.

Learn more

- Media and External Communications Policy
- Market Releases and Investor Relations Policy
- Market Disclosure Policy
- Social Media Standard
- Internal Communications Policy

Who to contact for help

Head of Investor Relations

Head of Group Communications

Communications Manager/Officer

In practice

Scenario	Response
At a weekend BBQ, I shared sensitive information with my sister. She's an equity analyst. The information hasn't been disclosed to the public yet. **What should I do?**	If you think you've released sensitive information that hasn't been disclosed to the public, you must immediately report it to Investor Relations, a Disclosure Officer or the Company or Deputy Company Secretary.
At an industry presentation a colleague put up a slide that included a photo of the new block cave we're working on at site. I'm pretty sure we haven't notified investors. **What should I do?**	This may be material information that hasn't been disclosed to the public. You must immediately report it to Investor Relations, a Disclosure Officer or the Company Secretary.

We do

- Follow laws and Newcrest policies about external communication.
- Make sure any authorised public communication is clear, timely, fair and consistent.
- Avoid disclosing or publishing confidential company information.
- Respect confidential information and copyright laws.
- Make sure we know what our local site requirements are and follow them. Local sites may control the use of mobile phones, taking photos, video and audio recordings.
- Tell our line manager if we're going to an industry or networking event or if we've been asked to speak at an external meeting.

We don't

- Make public statements on behalf of Newcrest, unless we're an authorised spokesperson.
- Share material information unless we're authorised to do so.
- Use Newcrest trademarks or branding unless we have the appropriate permission.
- Speak to the media about Newcrest without first talking to Group Communications.
- When making a public disclosure, hide facts or leave out relevant information.
- Speak at an event on Newcrest's behalf without the guidance, support and approval of Group Communications.

Social Media

Social Media is no different to all other external communications about or referring to Newcrest. We take care to communicate in accordance with our values.

Our policies and standards for external communication also apply to social media.

Social media gives us the chance to share our story with people outside the company – our communities, our investors, our industry peers, governments and potential employees. It's important that we do this responsibly.

Our expectations of our people

You're empowered to speak positively about Newcrest on social media. We encourage you to interact with our official posts by liking, commenting and sharing.

If you want to share Newcrest information on your own personal social media account, you're strongly recommended to take a common-sense approach. Remember that your comments, likes and shares are public for all the world to see. Even if you don't mention Newcrest in your posts, they may still give the impression that they represent the company. This could be because Newcrest is mentioned in your bio or you wore a Newcrest branded shirt in a posted photo.

Make sure you understand the difference between what you can share in public and the role of authorised spokespersons. Don't discuss any confidential or sensitive information about Newcrest on social media. Consult the Social Media Standard, your line manager or Group Communications if you're unsure.

Establishing new external groups, sites or pages using the Newcrest name or logo is not permitted without the right approvals. Establishing accounts using Newcrest's name or logo can harm Newcrest's reputation. You could also undermine Newcrest's official social media channels. Only official Newcrest social media accounts can use Newcrest logos, trademarks and other intellectual property. Contact Group Communications if you see unofficial accounts using Newcrest or joint venture brands.

Make sure you read and understand our Social Media Standard. Speak to your line manager or Group Communications if you're unsure.

Learn more

- Social Media Standard
- Media and External Communications Policy
- Information Technology and Data Management Policy
- Workplace Behaviour Standard
- Privacy Policy

Who to contact for help

Your line manager

Group Communications Team

In practice

Scenario	Response
I saw a post on Facebook about something taking place at site that I know isn't true. **Can I make a comment to correct the information?**	No. Unless you're an authorised spokesperson, you aren't permitted to comment on Newcrest's behalf. Report the post to Group Communications.
I took a great photo of my teammates on-site with our open pit in the background. Everyone is in full PPE. **Can I post this on Facebook?**	Each site has its own rules around photography. Ask your line manager about the rules for your site. You also need to ask your teammates if they're okay with their photo being posted on social media.

We do

Interact with Newcrest's official posts by liking, commenting and sharing.

Talk about the parts of work we enjoy on social media. For example, taking part in a fundraising event at work, attending an industry conference or sharing published industry research.

Respect the privacy of people at work, customers, business partners and communities.

Make sure our social media profile and posts are consistent with how we present ourselves at work.

Take care when asking colleagues at work to be 'friends' on Facebook or Instagram.

LinkedIn is a good place for connecting professionally with work colleagues.

Make sure our personal use of social media during work hours doesn't distract us from our job or stop us from delivering our work.

We don't

Use our Newcrest email address to register on social media platforms for personal use.

Publish or disclose confidential or sensitive company information.

Create our own Newcrest social media accounts.

Respond to questions or negative comments on official Newcrest social media accounts, unless we're authorised.

If we see comments that need a response, we send them to Group Communications.

Speak negatively about our workplace on social media.

Regardless of our privacy settings, our posts can get shared publicly. Even after a post has been deleted, it can be tracked back to the person who posted it. Anonymous and closed group posts can also be tracked back to the person who posted them.