Helpdesk Call Ref. [   ]   MAR03 (North Division)

	Request for Access to Staff Monitoring Data **This form is to be used in the incidence of a** **Manager requesting access to staff monitoring data** **relating to customer service standards in emails** **using the 'Direct Reporting'Tool.**

Manager Name:	
Department:	
Ext. No:	Date:

Request for access to Staff email Inbox and Sent Items (please name staff members)	

Have you informed the member(s) of staff you are making this request?	Yes	
Unless you confirm staff have been informed you cannot proceed with this request		

Reason for request to access information:

Please now seek authorisation. Authorisation is required from your local Advertising or Commercial Director

Authorisation	Name	Signature	Date
Commercial/Sales Director			

Request Approved / Rejected (please circle as appropriate)

Once authorised please return this form to the Group IT Helpdesk

v. 1.0   July 2009

Procedure for monitoring staff email for Customer Service purposes

These guidelines have been devised for the routine monitoring of staff emails for customer service and training purposes only, using the 'Direct Reporting' tool provided by the company.
The system allows managers to request an email or multiple emails to be forwarded to the managers Inbox. The system will only allow access to an employee's Inbox and Sent Items folder. Any emails requested will be flagged in the user's mailbox identifying that the manager has requested a copy.

- Monitoring of staff emails by line managers can be achieved by logging a request with Group IT to create a "Manager's Access Group" using form MAR03.
- Individuals must be notified in advance that their emails are going to be monitored and the purpose for that monitoring i.e. "I will be monitoring your Inbox/Sent items next month as part of a customer service exercise, maintaining standards of communication with customers and for training/quality control purposes." Managers must re-issue the "Think before you Click" leaflet (available from the Group Data Protection Manager/HR) to the relevant staff as a reminder.
  However, employees should be warned that if, as a result of the monitoring, a breach of company policy is discovered, then further monitoring may take place as part of any potential disciplinary procedures.
- If a breach of the Group IT Acceptable Use Policy is identified during the monitoring, then the manager must inform the Divisional HR Director immediately, for further investigation to take place.
- All email users must be reminded that any personal emails must be marked as 'PERSONAL' in the subject line.
- Managers must not request emails marked PERSONAL or any folders marked as PERSONAL.
- If a manager opens an email marked PERSONAL in error then the employee should be advised accordingly.
- Managers must only select emails to be forwarded to their inbox for customer care/quality control purposes. When monitoring, managers must remember their obligations under the Data Protection Act and Human Rights Act as employees have rights to privacy under this legislation even when using company equipment.
- Managers must not forward any monitored emails to other members of staff other than HR.
- Any monitoring for potential disciplinary purposes must be requested via a Management Access Request (MAR01) which has been approved and signed by a director and the Divisional HR Director.
- It is the responsibility of the line manager to ensure their 'Manager's Access Group' is kept up to date.

Manager's Guidelines to Delegated Access

What is Delegated Access?
Delegated access is a method by which a manager or nominated senior member of staff can access another employee's email inbox when a business critical email has been sent to the employee and the employee is unable to access it, for example, due to sickness or holiday. This form of access has been developed in the interests of business continuity and should not be used to monitor employees or to obtain evidence for employee disciplinary purposes.

How does it work?
The access is through the manager's username and password. Under no circumstances should the employee be asked to disclose their password to their manager or colleagues. This would be in breach of the Data Protection Act and the IT Acceptable Use Policy.

DO	DO NOT
Only open business related emails that you need to for the purpose in mind	Open any emails marked PERSONAL in the subject line
Let the employee know if you open one of their PERSONAL emails in error	Open any folders marked PERSONAL
	Use delegated access as an opportunity to monitor your staff
	Ask employees to tell you their passwords

What happens if I see something which I think is a breach of policy and needs further investigation?
All investigations must be conducted within strict guidelines to ensure compliance with the Data Protection Act and the Human Rights Act. Any suspected breaches of Johnston Press policy or disciplinary issues must be notified to your Divisional HR Director. They will risk assess the situation and arrange for further investigation which may include more detailed monitoring of emails or Internet usage to be conducted in line with Johnston Press disciplinary procedure. You will not be given open access to monitor an employee's email account.

Any manager who is found to be abusing their delegated access rights to their employee's inbox will be considered as being in breach of the IT Acceptable Use Policy and may be subject to a disciplinary investigation.

IT Acceptable Use Policy: http://jp/?id=307#TOP

Created by SPILKINGTON

Johnston Press Plc, the publishers of your local newspaper & website, take great care to ensure that important matters such as compliance with the Privacy Regulations are properly managed. We take our responsibilities for our customers' personal information very seriously and work hard to safeguard your privacy at all times.

Our Cookie Policy

How Johnston Press Plc use cookies and what they are:

What is a Cookie?

Cookies are small data files which are sent to your browser (Internet Explorer, Firefox, Chrome etc) from a website you visit. They are stored on your electronic device.

What is a Flash Cookie?

This is a type of cookie which is collected by Adobe Flash media player (it is also called a Local Shared Object) – a piece of software you may already have on your electronic device to help you watch online videos and listen to podcasts.

Can I opt out of receiving cookies?

Yes there are a number of options available, you can set your browser either to reject all cookies, to allow only "trusted" sites to set them, or to only accept them from the site you are currently on.

However, please note – if you block/delete all cookies, some features of our websites, such as remembering your login details, or the site branding for your local newspaper may not function as a result.

The types of cookies we, our ad network and technology partners use are listed below:

Revenue Science. (.revsci.net)

A tool used by some of our advertisers to target adverts to you based on pages you have visited in the past. To opt out of this type of targeting you can visit the 'Your Online Choices' website by clicking here.

Google Ads (.google.com)

Our sites contain advertising from Google; these use cookies to ensure you get adverts relevant to you. You can tailor the type of ads you receive by visiting here or to opt out of this type of targeting you can visit the 'Your Online Choices' website by clicking here.

Webtrends/ Google Analytics (.webtrends.com / statse.webtrendslive.com)

This is used to help us identify unique visitors to our websites. This data is anonymous and we cannot use this to uniquely identify individuals and their usage of the sites.

MOD100049336

Dart for Publishers (.doubleclick.net)

This comes from our ad serving technology and is used to track how many times you have seen a particular ad on our sites, so that you don't just see one advert but an even spread. This information is not used by us for any other type of audience recording or monitoring.

ComScore (.scorecardsearch.com)

ComScore monitor and externally verify our site traffic data for use within the advertising industry. Any data collected is anonymous statistical data and cannot be traced back to an individual.

Local Targeting

Our Classified websites (Photos, Motors, Jobs and Property Today) use cookies to ensure you get the correct local newspaper branding and content when you visit them. These cookies store no personally identifiable information.

Grapeshot (www.grapeshot-media.net/.grapeshot.co.uk)

We use Grapeshot as a contextual targeting technology, allowing us to create custom groups of stories outside out of our usual site navigation. Grapeshot stores the categories of story you have been exposed to. Their privacy policy and opt out option can be access here.

Subscriptions Online (.subscriptionline.co.uk)

Our partner for Newspaper subscriptions online stores data from the forms you complete in these to increase the usability of the site and enhance user experience.

Add This (.addthis.com)

Add This provides the social networking widget found in many of our pages. This widget gives you the tools to bookmark our websites, blog, share, tweet and email our content to a friend.

3rd Party Cookies

We use Advertising agencies to provide us with some of the advertising on our websites. These include (but are not limited to) Specific Media, The Rubicon Project, AdJug, AdConion, Context Web. Please click on the provider name to visit their opt-out page.