Guidance

BYOD Guidance: Good Technology

Published 16 March 2015

Contents

1. About this guidance

1.1 Who is this guidance for?

This guidance is for UK Public Sector organisations, their agencies and their suppliers who are considering deploying Good for Enterprise and/or Good Dynamics - collectively referred to as Good-enabled applications. It is written for system administrators and information risk owners responsible for deploying End User Devices (EUDs) for remote working at OFFICIAL.

Readers are expected to be familiar with the operation and functionality of Good for Enterprise and/or Good Dynamics in addition to the EUD Platform Security Guidance and BYOD guidance, which this guidance builds on.

1.2 What is Good for Enterprise?

GFE is an application suite which aims to protect a device's email, contact information and calendar, in addition to providing a secure browser and camera. This is done by creating a corporately-managed container that allows technical controls to be enforced in the absence of ones provided by the underlying platform.

GFE and GD also support mobile device management (MDM) although this not been

assessed.

1.3 What is Good Dynamics?

GD refers to two similar solutions from Good Technology; a Software Development Kit (SDK) and an application 'wrapping' toolkit.

The SDK can be used by independent software vendors (ISVs), as well as Good Technology, to create mobile applications. GD-secured applications are able to take advantage of the storage and networking APIs provided by the SDK (instead of the native platform) to encrypt data-at-rest and data-in-transit. The SDK also provides an organisation with controls over specific application behaviour, such as copy-and-paste functionality and data transfer between applications.

When using the wrapping toolkit, Good Dynamics provides a subset of the SDK features by modifying the application binary after it has been compiled to make use of the GD APIs. This does not require any code changes by the application developer.

2. Summary of key risks

In addition to the common risks of unmanaged hardware the following significant risks have been identified:

1. Without confidence in the underlying platform, applications cannot add extra security. If a device is compromised by malware then the protection offered by Good-enabled applications could be circumvented and sensitive information would be accessible. For this reason it is important to ensure that appropriate protection is provided to the device as a whole, as well as to applications.
2. Apart from Direct Connect traffic, network data transferred from Good-enabled applications is routed via the Good Network Operations Centres (NOCs) located in the United States. User data is encrypted such that it is not accessible to the NOC even with priviliged network access. However some metadata about the organisation is accessible which would permit attackers with privileged network access to discover:
   - GFE-registered users' email addresses
   - which organisation a device is registered to
   - which Good-enabled applications are installed on devices
   - the Active Directory domain name(s) that the GMC, GMM, GC and GP servers are connected to
   - the Active Directory user account name used to set policy on the GMC control panel
3. The GFE client is contained within a single sandbox; there is no isolation between

internal components (such as the email client and web browser). An adversary who is able to exploit a vulnerability in one component would be able to access all data stored within the GFE client. When using the GFE client as the Authentication Delegate (for single sign on) this would also include the encryption keys for GD-secured applications.

In addition, if the application wrapping functionality of GD is used, the following also applies:

The process of converting regular applications into wrapped applications has not been fully assessed, and there are a number of residual risks. There might be some APIs that write data onto the device that are not wrapped, which would leave unencrypted data on the device. Supplying a malformed application to the wrapping process might lead to incorrect or incomplete wrapping, or potentially compromise the wrapping server. The process of wrapping an application and then requiring the original developer to re-sign it leaves scope for the wrapped application being modified (intentionally or otherwise). This risk is not limited to GD, as it applies to any application wrapping approach.

3. Architectural components

Good for Enterprise and Good Dynamics consist of several components. Installation and configuration guidance for GFE and GD is available from Good Technology. This section discusses how an organisation can align this with both the EUD Platform Security Guidance and the Walled Garden Architectural Pattern (which eligible organisations can obtain from CESG).

3.1 Good for Enterprise components

GFE consists of five components:

- Good for Enterprise client application (installed on an EUD)
- Good Technology's NOC
- Good Mobile Control (GMC) server
- GMC database
- Good Mobile Messaging (GMM) server

The GMC server manages users, devices and policies while the GMM server acts as a relay between the GFE client and the corporate email service. The GMM server also proxies web traffic from the GFE client to intranet web applications. The GMC database is an SQL database that stores all policy, configuration and container information. The database can be installed on the GMC server or a separate SQL server. Organisations can deploy multiple GMC and GMM servers for load balancing.

3.2 Good Dynamics components

Good Dynamics consists of six components:

- the Good Dynamics SDK
- an application built with or wrapped with the Good Dynamics SDK
- Good Technology's NOC
- Good Control (GC) server
- GC Database
- Good Proxy (GP) server

The GC server manages users, devices, policies and GD-secured applications while the GP server is used to route network traffic from GD-secured applications to internet and intranet services. The GC database is an SQL database that stores all policy, configuration and container information. The database may be installed on the GC server or a separate SQL server. Organisations can deploy multiple GC and GP servers for load balancing.

3.3 Common principles

Where possible, organisations should reuse existing infrastructure rather than install duplicate systems solely for GFE and/or GD. Network traffic between the Good NOC and the GFE / GD servers installed in the corporate network should be routed through existing protective monitoring solutions.

The underlying server platforms should be configured in accordance with good practice, such as ensuring timely patching and creating accounts with the minimum necessary privileges. Access to critical configuration files should be restricted so that sensitive settings are protected.

As part of giving accounts the minimum necessary privileges, the Windows service accounts required for the GFE and GD corporate servers (the 'GoodAdmin' account by default) should be prevented from logging into workstations. While more complex to initially configure, using Managed Service Accounts (available from Windows Server 2008 R2 onwards) can simplify service administration and provides increased security over that provided by a Domain User account.

Digital certificates used by the GFE and GD servers installed in the corporate network should ideally be chained to the organisations's existing Certificate Authority, and appropriate access controls should be applied to protect private keys.

Unless using DirectConnect, no inbound firewall exceptions are required on the external firewall as the GMM and GP servers initiate outbound TLS connections to the Good NOC.

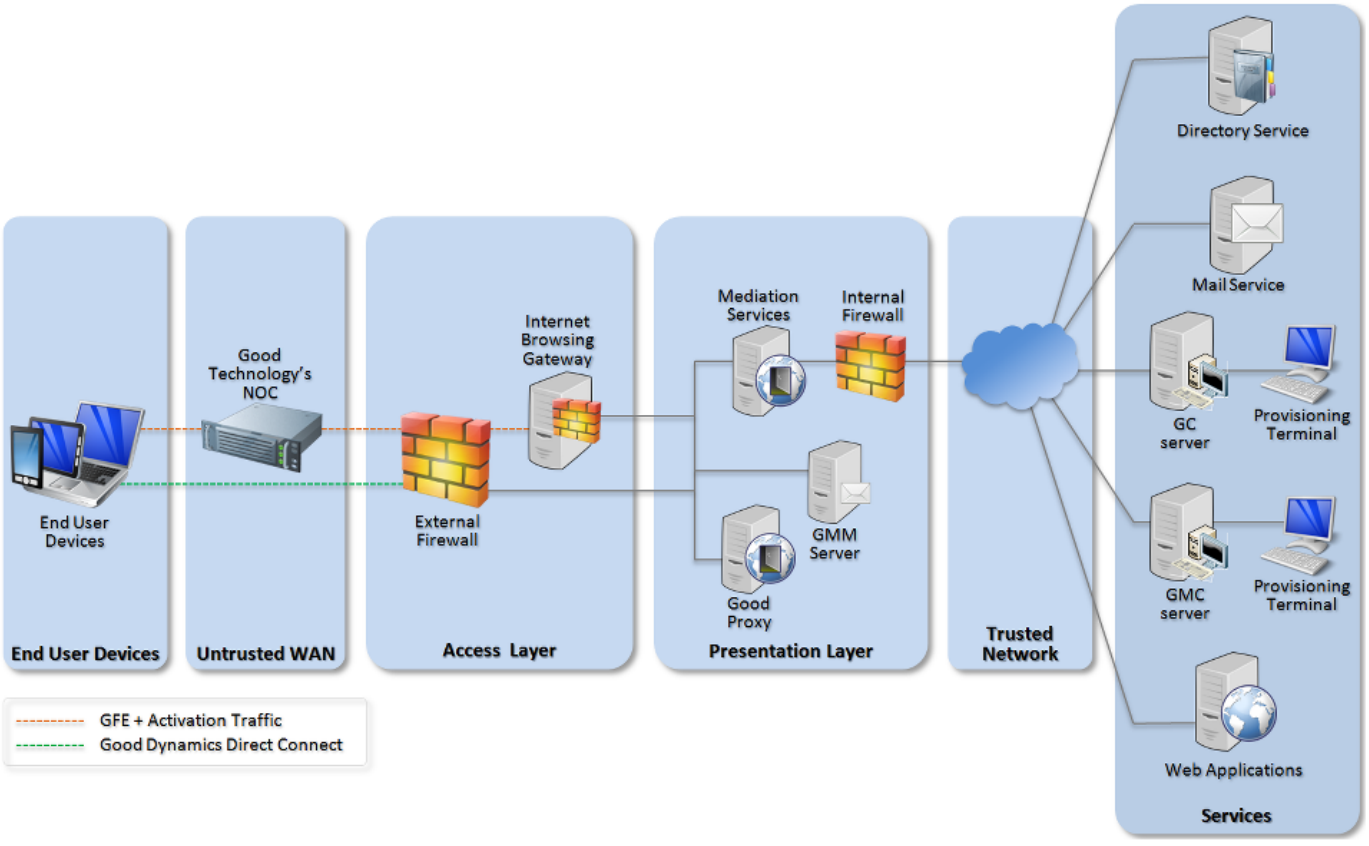
Outbound firewall rules should be added if necessary.

3.4 Recommended network architecture

This architecture aims to limit the impact of a compromise of an EUD and isolate high risk components from high value components where possible.

The servers installed into the corporate network as part of GFE and GD are high value resources that require suitable protection but are also high risk; they perform complex processing tasks that are more likely to contain exploitable vulnerabilities. These competing properties make securely placing the servers into an existing network challenging and organisations that wish to deviate should ensure they understand the risks of doing so.

Since GFE and GD are architecturally similar, components from both solutions are represented on a single diagram and discussed in parallel. Where the solutions differ, this is highlighted.



Recommended network architecture for deployments of Good for Enterprise/Good Dynamics

Unless “Direct Connect” is used, network traffic from the GFE client and GD-secured applications is routed to the Good NOC. The GMM and GP servers each maintain a

persistent TLS connection to the NOC which the NOC uses to route traffic. So that the NOC cannot access user data, it is further encrypted with keys not known to the NOC.

As network traffic is encrypted between EUDs and the GMM / GP servers, protective monitoring solutions will not provide meaningful results unless analysing traffic that has been decrypted on the GMM / GP servers.

The GMM and GP servers should be deployed in the presentation layer of the corporate network to minimise the exposure of core networking services and limit access to those services that are explicitly required for GFE and GD to function. The GMM and GP require access to application servers, such as email. Where possible, organisations should make use of existing mediation services in the presentation layer (such as a reverse proxy or mail edge transport server) rather than add additional firewall rules to the internal firewall to permit access to services within the core network.

The GMC and GC servers should be deployed in the core of the corporate network to protect them from malfeasance. Firewall rules will need to be added to the internal firewall to allow the GMM and GP to communicate with the GMC and GC servers.

4. Technical assessment

4.1 Summary of application security

The EUD Security Framework describes twelve areas for security controls for devices, each of which should be considered when deploying a particular solution. The EUD Platform Security Guidance goes on to detail how several specific platforms meet or fall short of these controls.

Organisations should consider the common risks of using unmanaged devices in addition to specific risks highlighted in this guidance.

The following table highlights how using GFE and/or GD improves or weakens the 12 principles on an EUD configured in-line with the guidance, although these only apply to Good-enabled applications rather than the whole device. Further technical details are provided in the following sections. Blank lines indicate no signficant changes to the protection provided by the underlying platform.

Security principle	Impact
1. Assured data-in-transit protection	The GFE/GD client enforces end-to-end encryption of data-in-transit that cannot be disabled by an end user but this has not been independently assured to Foundation Grade. GD-secured application developers can opt out of data-in-transit protection.

2. Assured data-at-rest protection	GFE and GD encrypt all application data although this protection is reliant on the native platform data protection mechanisms.
3. Authentication	Additional authentication of interactive users can be enforced to control access to GFE/GD application data.
4. Secure boot	
5. Platform integrity and application sandboxing	The GFE client is contained in a single sandbox such that a compromise of one internal component could give access to all protected data. GD-secured applications are reliant on the platform's underlying sandboxing mechanisms.
6. Application whitelisting	Organisations control provisioning of Good-enabled applications and can control which of these applications can share information.
7. Malicious code detection and prevention	GFE and GD provide jailbreak detection, although software on a compromised device cannot reliably provide proof of no malware.
8. Security policy enforcement	Administrators can set various information management policies within GFE and GD-enabled applications, which users cannot override.
9. External interface protection	
10. Device update policy	The GFE client and GD-secured applications can check compliance against organisational policies and can lock or wipe themselves.
11. Event collection for enterprise analysis	The GFE and GD corporate servers provide limited information for analysis.
12. Incident response	The GFE client and GD-secured applications can be configured to lock or wipe themselves if an incident is detected.

4.2 Data-in-transit protection

GFE and non-DirectConnect protected information from GD applications is sent to the Good NOC using TLS. The GMM and GP servers each maintain a persistent TLS connection to the NOC which the NOC uses to route traffic. So that the NOC cannot access user data, it is further encrypted with keys not known to the NOC.

Good-enabled applications transmit network traffic to the Good NOC using TLS. Using metadata in the traffic, the NOC identifies which organisation the traffic is destined for and forwards it using a separate TLS connection to the GMM or GP. In order to prevent the NOC accessing sensitive user data, application data is further encrypted using a

proprietary protocol. The encryption keys for this data are generated on the GMM server and not known to the NOC.

The encryption does not meet some of the mandatory requirements expected from assured TLS VPNs. Without assurance in the data-in-transit protection, there is a risk that data could be compromised.

The GFE client cannot circumvent the data-in-transit protection. GD-secured applications could be developed with the ability to directly communicate with Internet services, without network traffic being transmitted via the NOC. In such cases, the protection of this network traffic is dependent on the application's own functionality, not the GD framework.

For GD-secured applications, DirectConnect can be used to transmit application data directly to the corporate network, without transiting the NOC. Administrative actions, such as application provisioning and policy enforcement, are still routed through the NOC. Whilst this does not improve or weaken the data-in-transit protection, this can improve latency-sensitive applications.

> Recommendation: If confident that sensitive data will never be stored or accessed from outside the GFE client and/or GD-secured applications, and the risks of not protectively monitoring all device network traffic are acceptable, organisations do not need to deploy a device VPN.

4.3 Data-at-rest protection

Application data is stored in an encrypted container. This encryption has not been independently assured to Foundation Grade.

The encrypted container sits on top of the EUD filesystem therefore the security of the encrypted data on a device is linked to the strength of the user's GFE / GD passphrase(s) (users can have multiple passphrases for different GD applications) and the protection provided by a device passphrase. On iOS devices the container uses Data Protection class C which provides dedicated hardware protection. The GFE / GD passphrase(s) can therefore be reduced in length and complexity on iOS devices.

To avoid users being required to enter their passphrase every time they open an application, a timeout period can be configured by the organisation; sensitive user data is not protected during this timeout period. A shorter timeout period will decrease the opportunity for an adversary to access sensitive information but is likely to impact user experience.

Recommendation: The passphrase for GFE and GD-secured applications should be different from the device passphrase and handled in line with organisational policy. The EUD Platform Security Guidance contains advice on appropriate policy.

Recommendation: When deciding on an appropriate timeout period, departments should balance user experience against security. The timeout period should be no longer than 15 minutes.

4.4 Web content protection

The GFE client provides a web browser, known as Good Mobile Access (GMA). GMA protects browser, cookie and Adobe Flash data on the device by overriding the default platform storage methods with methods that make use of the GFE client's encrypted container. This data is not available to other applications unless they are built with Good Dynamics and access is permitted by policy.

GMA does not override the W3C Web Storage APIs (commonly known as HTML5 localstorage), which websites may use to store user data. This is also true for GD-secured applications which make use of these APIs or are built with HTML5 frameworks that make use of them. Information stored using these mechanisms is not protected. As with all web browsers, malicious or compromised websites may be able to exploit a vulnerability in GMA in order to access sensitive data.

Recommendation: Organisations should ensure that web applications accessed with GMA and GD-secured applications do not store sensitive data using the Web Storage APIs.

Recommendation: Good Mobile Access should be configured to only allow access to intranet websites and applications to limit the exposure to malicious websites.

4.5 Malicious code detection and prevention

Jailbreaking (or rooting) is the act of exploiting a vulnerability in the operating system to disable various security restrictions, typically to allow unofficial modifications or applications to be used. This is equivalent to what malware often tries to achieve.

Compliance management can be configured to report when it detects that a device has been jailbroken or rooted such as wiping the Good container(s). It can optionally be configured to prevent further access to Good-enabled applications or remove them from the device. Limitations of current technology mean that this ‘device status’ check is not sufficient to verify absence of malware; malware could subvert such a check.

Recommendation: Jailbreak detection should be enabled, but administrators should be aware of its limitations.

4.6 Document import and export

The GFE client and GD-secured applications can be configured to allow data to be imported and exported from other applications. These controls can help an organisation manage which applications are able to access sensitive data.

While an organisation may be more concerned with preventing documents being exported from these applications, it is important to remember that imported documents could contain malicious content. If they are transferred from the application to other corporate infrastructure, such as a file store, the malicious content may not be scanned and could attack the corporate network.

Recommendation: Configure policies to only allow GFE and GD applications to import data from trusted sources, such as white-listed applications or intranet locations.

Recommendation: If arbitrary document importing is permitted, ensure that imported documents are not able to circumvent existing protective monitoring solutions. The recommended network architecture is designed to limit the impact of such attacks on the corporate infrastructure.

4.7 Temporary Unlock Code (TUC)

Good-enabled applications can be unlocked via a temporary unlock code, which is generated during application provisioning and stored in the GMC or GC database. This unlock code is used to unlock the application in the event of a forgotten passphrase and should be protected to the same degree as the user passphrase. If an organisation is planning on allowing the temporary unlock code to be provided remotely by a help desk,

callers must be manually authenticated prior to providing the key.

4.8 GFE application sandboxing

To limit the information and functionality available to an application, many platforms provide an application sandbox. If an application is malicious or compromised, an adversary is unable to access information outside the sandbox without exploiting a weakness in the sandbox.

Since the GFE client is contained within a single sandbox, there is no isolation between internal components (such as the email client and web browser). An adversary who is able to exploit a vulnerability in one component would be able to access all data stored within the GFE client.

When using an application as the Authentication Delegate this data would also include the encryption keys for GD-secured applications such that the adversary could access all information protected by Good-enabled applications.

> Recommendation: Organisations should carefully consider what Good-enabled applications to install.

4.9 GFE address book synchronisation

The GFE client provides its own address book, which is stored within the GFE client. This data is not available to other applications unless they are built with the GD framework, and access is permitted by policy.

The GFE client can synchronise this contact information into the native contact store, for example to allow the platform to display the name of who is calling. Organisations can configure which information is synchronised (such as name, phone number, email address, notes, address etc.), permitting a more granular level of information disclosure.

> Recommendation: Organisations should consider which fields within the address book are sensitive, and configure the synchronisation policy accordingly.

4.10 GFE calendar alerts

The GFE client provides its own calendar, which is stored within the encrypted application container. This data is not available to other applications unless they are built with the GD framework, and access is permitted by policy.

When a reminder is set for a calendar appointment and this reminder is triggered, the GFE client triggers a device popup message. This message can either display the appointment details or use a generic alert instructing users to open the GFE client for actual appointment details.

> Recommendation: Organisations should consider whether calendar appointment information is sensitive, and configure the calendar alert policy accordingly.

4.11 GD application protection

Good Dynamics is designed to provide application developers with a cross-platform set of security features. The security offered by Good Dynamics is reliant on correct use of the framework by ISVs, although GD-secured applications are required to undergo testing prior to publication. This testing is designed to identify any errors in the use of the GD framework so it does not cover the application's business functionality, which may be otherwise insecure or malicious.

Good Dynamics can also be used directly to 'wrap' application binaries with minimal involvement from an ISV. This requires Good Technology to dynamically identify application code that is writing content to a disk or network and modify the behaviour to use the GD-provided functionality. There is a large and changing list of APIs that Good Technology must cover to ensure sensitive data is protected; failure to identify all the necessary APIs could result in data not being protected by GD. Wrapped applications can still contain malicious functionality.

> Recommendation: Administrators should not install arbitrary applications, even if built with the GD framework, and should still perform due diligence testing to satisfy themselves that applications do not contain malicious functionality.

4.12 GD framework updates

Updates to the GD framework are not applied to installed GD-secured applications directly. Applications need to be recompiled with the updated framework by the developers and then deployed to devices. Applications not using the latest version of the GD framework

may contain publically-known vulnerabilities that an attacker could exploit.

> Recommendation: Departments should ensure provisioned GD-secured applications make use of recent updates to the GD frameworks.

4.13 Network Operations Centre

Good Technology runs two NOCs in the United States that act as relays between EUDs and the GFE and GD servers installed in the corporate network. User data is encrypted using keys not known to the NOC.

The NOC's role as a communications broker between the EUD and the corporate network means that it helps to protect the exposed corporate services against a network attack. Despite this the NOC is still in a privileged position and is able to:

- prevent the relaying of network traffic between the client and corporate servers, denying service to users
- identify which devices belong to an organisation and what Good-enabled applications are installed
- access the metadata of network traffic, including:
  - GFE-registered users' email addresses
  - the Windows domain name(s) that the GMC, GMM, GC and GP are connected to
  - the names of user accounts used to set policy on the GMC control panel

> Recommendation: Organisations should understand what metadata is available to the Good NOC, identify whether it is sensitive and ensure they have sufficient trust in Good Technology to protect it. They should also establish that the service availability levels meet their requirements.

4.14 Mobile device management

GFE and GD can provide MDM functionality through the GMC or GC server. This functionality has not been reviewed and organisations should perform their own assessment as they would for any MDM provider.

Although the GMC server is installed within the corporate network and policies are configured locally, MDM profiles are stored in the Good NOC. The GFE MDM functionality should be treated as a cloud MDM service. Anyone with access to the NOC would be able to manage devices on behalf of the organisation, and could change security policies or

unlock or remote-wipe a device. They would also be able to recover provisioned credentials stored within an MDM profile.

> Recommendation: Organisations should ensure they have sufficient trust in Good Technology to manage devices on their behalf and protect the NOC from malfeasance.

4.15 Protection of the Over-The-Air (OTA) PIN

To activate the GFE client and GD-secured applications, users are issued with a PIN (respectively, the OTA PIN and GD access key). This PIN is generated by the GMC or GC server and registered against the provisioned user, although it is not tied to a specific device. The PIN can then be distributed to a user manually or via an automatic email.

For Good Dynamics, the PIN can only be used to provision one application on one device, it cannot be reused. The PIN can also be set to expire after a configurable time period if it is not used. For GFE, an expiry time can also be set however the PIN can be reused by default. Reuse can be disabled by policy.

For the security of the overall deployment, and to prevent information loss, it is important that the PIN be kept protected until it has been used by the legitimate user.

> Recommendation: The OTA PIN should always be handled in accordance with the classification of data that the application will handle. If the PIN is sent to a user by email, the user should be reminded of the importance of keeping it protected and not allowing it to be passed to others.

> Recommendation: Users must be trusted to use the PIN on the expected device or organisations should consider an Administrator provisioning GFE and/or GD-secured applications as part of a device provisioning process.

> Recommendation: Organisations should disable OTA PIN reuse for GFE. Easy Activation should be considered for GD applications, to reduce the likelihood of PIN compromise.

5. Other considerations

Prior to deploying GFE or GD-secured applications, a number of other risks should be further explored by organisations. These are covered below.

5.1 Security control availability

GFE and GD provide a range of controls that an organisation can make use of. Some of these controls apply to the GFE client or a GD-secured application while some are applied via the platform's MDM capabilities. Organisations should ensure they understand which controls apply to the GFE client and GD-secured applications, and which apply to the MDM functionality.

5.2 Logging

GFE and GD contain logging functionality that can report diagnostic information to Good Technology from the Good-enabled applications and supporting servers. Summary logs are generated by default but are not automatically shared with Good Technology.

Organisations should disable the sharing of log data with Good Technology unless they are confident log data does not contain sensitive data.

5.3 GMM server communications

The GMM server communicates with the corporate mail service. For Microsoft Exchange, it currently supports both the MAPI and EWS protocols. As a more modern protocol that requires less ports to be opened on the inner firewall, EWS is recommended over MAPI.

Legal information

fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it.