Data Protection Policy- GDPR
Protocol for Use

Guide for staff, partner organisations and service users

May 2018 Issue 8

Copyright ©

This document summarises the Company's policies, procedures and guidance for all members of staff working with FosterTalk in the UK (including self- employed workers) under the General Data Protection Regulation which comes into effect on 25th May 2018, replacing the Data Protection Act 1998.

Contents

Copyright ©
Produced by FT HR

Introduction

FosterTalk has an obligation under the General Data Protection Regulation (GDPR**)** to treat the personal data of individuals including carers, young people, employees, self-employed contractors, applicants for employment, interview candidates, former employees and agency workers with the utmost respect. Everyone in the workplace has a legal duty to protect the privacy of information of others. The GDPR applies to paper records as well as those held on computers and other forms of electronic media.

The FosterTalk Board of Directors wishes it to be known that it takes compliance with data protection legislation very seriously. Failure to adhere to the policy and additional guidance will be treated as a breach of policy and may result in disciplinary action being taken against the individual(s) concerned.

GDPR Principles

The GDPR sets out 7 principles for the lawful processing of personal data. These are contained in the following articles:

Article 5 Principles relating to processing of personal data
Article 6 Lawfulness of Processing
Article 7 Conditions of Consent
Article 8 Conditions applicable to child's consent in relation to information society services
Article 9 Processing of special categories of personal data
Article 10 Processing of Personal Data relating to criminal convictions and offences

Copyright ©
Produced by FT HR

Article 11 Processing which does not require identification

Chapter 2, Article 5 outlines the new principles as follows:

"Personal Data shall be;

1. *processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);*

2. *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes;('purpose limitation');*

3. *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

4. *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

5. *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 83(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*

6. *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality');"*

Individuals' Rights

The GDPR provides the following rights for individuals

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Privacy Statements

Copyright ©
Produced by FT HR

The right to be informed encompasses an organisation's obligation to provide "fair processing information" typically through a privacy notice. FosterTalk's Privacy Statement summarises the way the company gathers, uses, discloses and manages personal data and can be found on the company website. www.Fostertalk.org

Supporting procedures

This policy and accompanying guidance sets out FosterTalk's obligations in handling data under the GDPR and should be read in conjunction with the following policies:

- Code of Conduct
- Electronic Communications Policy
- Equipment and Access Protocol
- Reference Request Policy
- Subject Access Request Protocol
- Archive and Retention Policy and Procedure

Copyright ©
Produced by FT HR

Glossary of Terms

• **Authorised individual**	The person on which the data is held; an officially appointed representative of that person; or a co-worker (other than the data subject) who requires access to the personal data to do their job.
• **Data**	All electronic and paper records including pictures and video recordings
• **Personal data**	Data that can be linked to an individual, or gives information in some way about a person.
• **Live data**	When data is being used or shared on a regular basis, we define this as 'live data'. There are important issues regarding live data which include storage, accuracy and how the data is shared.
• **Data controller**	A person who is responsible for data protection in a company and is registered with the UK Information Commissioner (et al) as the accountable person.
• **Data Processor**	A person/ body who processes data on behalf of the data controller.
• **General Data Protection Regulation (GDPR)**	The GDPR applies in the UK from 25th May 2018. The government has confirmed that this will not be affected by the UK's decision to leave the EU. Further information can be found at www.ico.org.uk
• **Data subject**	A person whom personal data is being collected from, which could be a foster carer, employee, child being fostered; or some other person.
• **Data user**	An employee of FosterTalk who is responsible for collecting and guarding personal data as part of their work. This will generally be every employee, but some will do more than others and some will deal with particularly personal data
• **Data security**	The safeguards that FosterTalk has in place to prevent information from being lost or misused
• **Information**	Any reference to the word "information" in the context of data security shall mean the same as "data".
• **Inappropriate use**	Using data for purposes that fall outside the purposes defined in the GDPR. This could include sharing the information inappropriately, or failing to take adequate steps to ensure its safety.

Copyright ©
Produced by FT HR

Employee's/ workers' responsibilities

Workers have responsibility for data protection under the GDPR. Line managers have responsibility for the type of personal data they collect and how they use them. No worker should disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes. A worker disclosing personal data without the authority of the organisation may commit a criminal offence, unless there is some other legal justification for example under 'whistleblowing' legislation and may be subject to disciplinary action.

Personal data is subject to the General Data Protection Regulation in the UK. Under the terms of the GDPR, personal data includes any information about a living identifiable individual, including their name, address, telephone number and e-mail address. If you include such information in an e-mail or an attachment to an e-mail or fax, you are deemed to be "processing" personal data and must abide by the law.

In particular, the company and employee must not;

- collect personal data without the person's knowledge
- disclose or amend such information except in accordance with the purpose for which the information was collected
- use personal data for purposes other than those for which it may have been explicitly collected.
- Knowingly ignore or contravene safeguards that have been put in place regarding the storage and security of personal information.

Guide to security procedures in the workplace

FosterTalk shall ensure that facilities are available to data processors that help prevent viewing by unauthorised individuals in the form of physical and electronic locking devices; and data processors shall make use of those facilities; and employ good administrative practice to minimise the risk of unauthorised viewing. FosterTalk shall also ensure that reasonable measures are in place to minimise personal data loss, damage, theft or inappropriate use.

Secure lockable furniture

All paper-based records must be locked away when they are not in use, in desks, filing cabinets, or cupboards. Keys should be kept in a safe place and workers should adopt a clear desk policy.

Secure equipment

All workers should take special care with computer screens, fax machines and photocopiers.

- Place equipment appropriately within secure areas.
- Remove documents from photocopiers and fax machines after use.
- Make sure only authorised staff/workers can collect incoming faxes.
- When sending a confidential fax, ensure that the correct fax address is held, and that the receiving organisation is aware that a confidential fax is being transmitted.
- If printing confidential information to a photocopier ensure you use the 'locked print' facility if it is available
- Lock the computer screen whenever desks are unattended for a period of time.

Copyright ©
Produced by FT HR

- Change computer passwords every 30 days in line with the company's Electronic Communications Protocol
- Shut down computers at the end of the working day.

Electronic data

The following section should be read in conjunction with the Company's Electronic Communications Protocol.

Securing electronic data

If you are in possession of a laptop provided for you by the company you must take a common sense approach to securing/ storing your laptop when not in use.

- Do not leave your laptop in your car or unattended when travelling or visible on your desk when you are not working.
- Take care when storing confidential personal records next to high value electronic items
- Take care when travelling on public transport to ensure that you keep position of your device
- Ensure that security passwords for the laptop are not kept with the laptop.

You may be asked to replace a laptop at your own cost if it has been lost, stolen or damaged as a result of your negligence. If you do lose a device, you must report it immediately.

Removable media

The Company does not encourage the use of removable media for storing personal information about staff or FosterTalk members (e.g. memory sticks, CDs, DVDs, USB hard drives etc.) as they carry a risk to the organisation

However, in certain circumstances workers may be permitted to use removable media devices while on Company business, e.g. in order to carry out their role effectively. Only encrypted devices may be used. The devices should be password protected and the password kept in a safe place, and not near the device. When removable media is not in use it must be stored securely. Any loss or theft of a device must be reported immediately.

Please note: Any removable media issued by the Company forms part of the Company's equipment and should therefore be returned upon leaving the organisation

Reporting procedures for lost removable media

Lost or stolen media should be reported immediately to the Managing Director as this may constitute a breach of Data Protection legislation and could expose the company to significant fines in respect of breach of confidentiality, and distress or damage to data subjects.
See also: action to be taken in the event of a breach of this policy

Password protected documents

Any personal data pertaining to a worker or a member should be held securely and given password protection. All documents containing personal data must be password protected prior to being sent electronically to another worker. The password must not be shared within the body of the text containing the attachment.

Copyright ©
Produced by FT HR

Securing archive data

The GDPR operates with the requirement that the data subject's data be destroyed as soon as it is no longer required. However, this requirement has to be balanced with the need to retain certain data to meet other legal requirements, such as care standards, employment law or taxation.

The general requirement of this policy in relation to data no longer "live" shall therefore be to destroy it; or if retention is required (following an assessment made of what needs to be stored and why), To store it on the company database for no longer than required, except in exceptional circumstances.

Please refer to Archive and Retention Policy

Guide to retention of data

The company uses a Database whereby documents and other information can be stored electronically and accessed by staff that have relevant permissions. This limits the need for Shared drives/ folders. Data should only be retained for as long as necessary, and then deleted. Personal data must not be held on personal drives, but retained on the database and in shared folders where needed for specific reasons such as data analysis or mailings. Holding data in shared files ensures that the data can be appropriately secured, and accessed by staff who have a legitimate requirement.

Accuracy

Data processors have an on-going obligation to ensure data remains accurate and within the law. In practice this will mean processes and procedures are in place to periodically review the relevance and accuracy of personal data; and data that is found to be inaccurate or not required will be immediately destroyed.

Data controllers and processors may apply a degree of discretion on the issue of accuracy. For example, if a letter on file was headed with an out-of-date address, but the content remained relevant, then the data processor should be able to justify the retention of the document as long as the reason for keeping it is valid.

Where a member of FosterTalk staff or contractor becomes aware of a change to personal data, such as a change of name, address or other personal data, they have a responsibility to either update the record, or inform the person responsible for maintaining database records.

Statistical data

FosterTalk regards historical statistical data as an important component in determining future trends. The retention of anonymised data for statistical purposes is therefore permitted subject to any data that identifies an individual being removed or modified.

Employment Application Forms

Applications for non-successful candidates shall be retained within the HR department for 6 months following the closing date of the vacancy. At this point the application forms will be securely destroyed. Where copies of application forms are made as part of the interview process, they must be returned to Human Resources within 48 hours of the interview (please refer to the staff recruitment procedure).

Copyright ©
Produced by FT HR

HR files for employees/ workers

The following information for permanent employees can be held locally by the appropriate Senior Manager in a secure environment in accordance with the GDPR, and may be used for the following purposes; supervision, learning and development, managing performance, and in responding to reference requests. Skeleton HR files must be kept in a secure lockable cabinet and only accessed by authorised personnel.

Local files should consist of the following:

- basic personal information sheet (provided by HR) which includes next of kin details
- job description/person specification
- annual leave card
- supervision notes
- Performance and Development Review documentation
- record of training/ personal development plan

Line Managers at FosterTalk should regularly review their local HR files to ensure the information is up to date and relevant. Any information which is irrelevant/ out of date or is duplicated with records held by HR should be securely destroyed. Information should not be held where there is no genuine business need for it or no legal duty to retain it.

Any correspondence written locally in relation to the employee must be forwarded to HR to be placed on the Central file. Once an employee leaves the Company any information stored on the local HR files should be forwarded to the HR department within 60 days of their departure to be archived with the HR file and any duplication of data will be destroyed.

Self Employed contractor Files

Self Employed contractor files shall be retained (in secure conditions) for a period no longer than 12 months following the conclusion of the tasked assignment/ contract for services, at which point they will be destroyed.

Agency Workers Records

The employment agency will keep records of any agency workers used by the Company. Any records kept by the Company should be filed in the name of the agency and in date order. Once an agency worker has not been active for 12 months, their records will be destroyed.

Guide to destruction of personal data

Personal data, regardless of whether it is live or archived, shall be destroyed responsibly as soon as retention cannot be justified. All workers must utilise safe methods for destroying papers, i.e. by shredding. The Company shall ensure that each office base has facilities in place for data destruction and on their part employees/ workers shall make every effort to use those facilities. No confidential paper records may be placed into general waste paper bins or into recycling bins without being shredded.

Copyright ©
Produced by FT HR

Archiving

Once an employee or casual worker leaves the Company, their personnel file is retained for 12 months (in lockable archive cabinets) in case it needs to be accessed for references or further information pertaining to the worker. After 12 months the file will be securely archived. After 6 years the file will be recalled to be safely destroyed. Payroll files will be kept for 6 tax years following an employee/ casual worker leaving the Company, after which point they will be securely destroyed.

Electronic Data

Electronic information shall be held by the Company in accordance with policies identified for manual records/ hard data. Employees should not use their personal computers for company emails, or their company computers for personal emails. They must ensure that emails are not retained longer than the purpose for which they were collected, and are held in such a way that they can easily be identified, reviewed and when necessary, destroyed.

Any unused or obsolete computer equipment must be returned to the IT Department so that it may be disposed of correctly and any data deleted securely.

For more information/guidance please refer to the FosterTalk Electronic Communications Protocol.

Employees and casual workers

Once the employee or casual worker leaves the company their electronic details on the HR database are set to 'archive'. The HR department shall ensure that employment records are retained for statistical purposes only and HR shall ensure that any data that identifies an individual is removed or modified and any out of date or irrelevant data is removed.

Guide to releasing data/ sharing information/ handling enquiries

Data processors shall understand who they are permitted to share their data with (authorised individuals) and whether the data needs to be filtered before being shared with a third party. All members of staff/ workers will be provided with training in responding to a request for information. Requests for personal data must be restricted to what is absolutely necessary for the task in hand and individuals should understand the reason why personal data is being collected.

See also Subject Access Request Policy and Guidance.

Telephone enquiries

Remember the following.

- Do not give out any personal information over the phone. The person's details should be taken and a call back arranged to ensure that their personal details and identity can be checked before proceeding with a subject access request.

- Never give out information about another person. For example, you should not give friends or relatives of employee/workers their address details

Copyright ©
Produced by FT HR

- Do not be bullied into giving information. The person requesting the information may not be who they say they are.

- No information will be given verbally, all subject access requests must be responded to in writing. Refer to Subject Access Request guidance (Appendix 1) for further information.

Releasing data overseas

The GDPR imposes restrictions on the transfer of personal data outside the EU, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR, which states that transfers may be made where the commission has decided that the third country or international organisation ensures an adequate level of protection.

Please refer to Human Resources for further information.

Releasing data for inspections and tenders

If personal data is requested for regulatory body inspections or for tendering purposes the employee, where reasonably possible or practical, will be contacted in order to gain their consent. Contents of personnel files shall only be released to authorised personnel. HR will keep a record of any files that are called away from the office and ensure they are returned at the appropriate times.

Guide to accessing information

Data processors should ensure that requests for personal data are restricted to what is absolutely necessary for the task in hand. Individuals should understand the reason why personal data is being collected.

Subject access requests

The GDPR grants employees/ workers/ service users/ customers the right to have a copy of the information that the company holds about them. The GDPR allows for any individual to make a 'subject access request' to the Company, verbally or in writing (letter or email) The Company must respond promptly and at the latest within one month of receipt of the request, providing copies of the information it holds, where it is reasonable to do so. Where requests are complex or numerous, the compliance period may be extended by a further two months. If this is the case, the individual must be informed within one month of the reasons for delay.

For more information on how to satisfy subject access requests please refer to Subject Access Request Policy and Procedure. Appendix 1.

All staff and contractors must be aware that

- Individuals have the right to make a subject access request
- Know to whom a subject access request should be addressed to within FosterTalk or be able to give an individual further information on how to make a request
- Be able to identify a request and pass it onto the right person within FosterTalk for response as soon as a request is received.

Copyright ©
Produced by FT HR

- Be aware of the exemptions that allow organisations to withhold information if necessary.

Exemptions:

Exemptions can apply in areas such as legal obligation, criminal investigation, defence of legal claims, management planning such as promotion and transfer plans, and negotiations. The exemptions, though, are limited in their application even within these areas. Care must also be taken in deciding whether or not to release information identifying 'third parties' i.e. people, other than the individual who has made the subject access request. Third party information can be redacted in certain circumstances.

The Right of Erasure

In addition to the right to make a subject access request and to have a copy of their personal data, data subjects have the right to withdraw their consent to their data being processed, to request that their data is deleted and/or to request that disputed data is rectified or amended.

All requests for the erasure or rectification of data will be respected and actioned in accordance with this Policy with the exception of the areas identified under “Exemptions” above.

Freedom of Information

The Freedom of Information Act 2000 (FOI) gives a person the right to ask any **public body** for any information they have on a particular topic, subject to certain exceptions. The authority is obliged to respond within 20 working days. Local authority contracts entered into by FosterTalk will invariably contain a clause requiring FosterTalk to pass on any request received and may require the provision of information to allow a response to be made. In the event a request for information is received it must be referred to the Managing Director immediately upon receipt to ensure it is sent to the relevant authority within the specified timescale.

The FOI Act also applies when submitting a tender. Certain information submitted to public bodies can be classed as ‘confidential’ or ‘commercially sensitive’ which could prevent it being released in the event of a future request for information. An authority will usually supply a form for submission within the tender documents.

Correspondence shared with local or central government departments may also fall under the scope of the Freedom of Information Act if held by a public body. Sensitive or confidential information shared should be clearly indicated as such.

Environmental Information Regulations 2004

Members of the public can apply to a **public body** for environmental information under the above regulations, a response to which must be made within 20 working days. As for the Freedom of Information Act above, FosterTalk should ensure any request received is passed to the relevant authority without delay and therefore any employee in receipt of a request must pass it to the Managing Director immediately.

Copyright ©
Produced by FT HR

Unauthorised disclosure/breach of data security

Organisations which process personal data must take appropriate measures to guard against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data.. The measures taken by FosterTalk are contained in the Data Protection Policy and Protocol.

In the event of a breach of data security, however minor you consider it to be, you must report this immediately to your line manager and/or the Managing Director.

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored (laptops, removable media, mobile phones)
- Unauthorised access to data (files left open, weak passwords, equipment left unlocked/unattended)
- Equipment failure
- Human error, such as information being sent to the wrong recipients.
- Unforeseen circumstances, e.g. fire or flood
- Hacking attack
- "Blagging" offences e.g. where information is obtained by deceiving the organisation which holds it.

However the breach has occurred, there are four important elements to managing it. These are:

1. Containment & recovery
2. Assessment of ongoing risk
3. Notification of the breach
4. Evaluation & response

1. Containment & recovery

Data security breaches require not just an initial response and investigation but also a recovery plan and where necessary action on damage limitation. This may require action across the business, e.g. IT, HR, Finance, admin and contact with external stakeholders.

The Managing Director will decide who should take the lead in investigating the breach and ensure the appropriate resources are available to them. They will also decide if other procedures should be invoked, e.g. disciplinary procedures.

The Managing Director will also establish who needs to be made aware of the breach, what action must be taken and by whom, and consider how best to limit any damage caused by the breach to third parties or the company.

2. Assessment of Ongoing Risk

Before deciding on what steps may be necessary beyond immediate containment, an assessment must be made of the risks associated with this breach. Most important is an assessment of potential adverse consequences for individuals or organisations, how serious or substantial these are, and how likely they are to happen again.

Copyright ©
Produced by FT HR

The following points should be considered:

- What type of data is involved?
- Is data still being lost, and how can further loss be prevented?
- What has happened to the data? (when and how was it disclosed?)
- How sensitive is it? (what is the potential for misuse?)
- If data has been lost or stolen, was it encrypted?
- If lost or stolen, could it be used to harm individuals?
- How many individual's data has been affected by the breach?
- Who are the individuals whose data has been breached? (staff, customers, etc)
- What harm could come from the breach?
- Are there wider consequences, including loss of business reputation?
- How can a repetition be prevented?

3. Notification of the Breach

Informing people and organisations that a data security breach has occurred is an important element in FosterTalk's breach management strategy and a means of maintaining confidence in the organisation.

The Managing Director will consider carefully who needs to be informed about the breach and who should carry out this role. Matters to be considered may include:

- Any legal or contractual requirements. E.g. does a service commissioner need to be informed?
- If equipment has been lost or stolen, do the police need to be informed?
- Will notification help the individual? E.g. by changing a password, or cancelling a credit card?
- If a large number of people are involved, what is the best way to communicate with them?
- How much information about the breach should be shared with them?
- If a large number of people are involved or there are likely to be serious consequences, the Information Commissioner may need to be informed. Further guidance is available on the ICO website at. https://ico.org.uk

4. Evaluation & Response

Once the investigation has been concluded**,** It is important to evaluate the causes of the breach and also the effectiveness of the company's response to it. If the breach was caused by inadequate policies, or lack of clear roles and responsibilities, then relevant policies and lines of accountability should be reviewed. A further review of systems and processes for managing personal data may also be warranted.

If human error, then disciplinary measures may need to be considered alongside further supervision, support or training for the individual concerned.

The learning from the data security breach should be shared with relevant staff members in order to raise awareness of potential risks and issues and prevent a recurrence.

Copyright ©
Produced by FT HR

See Also Checklist for Independent Workers/Contractors "How to Comply with Data Protection Requirements"

Review of Policy and Procedures:

This Policy was reviewed in May 2018 and will be reviewed annually or in line with any changes to legislation.

Appendix 1 - How to satisfy Subject Access Requests

Copyright ©
Produced by FT HR

What information is a person entitled to request?

An individual is entitled to see their own personal data and not information relating to other people (unless they are acting on behalf of that person, see below).

This right relates to information held at the time of the request and not necessarily a right to see the documents that include that information, though full consideration should be given to the wording of the request.

Although in most cases it will be obvious whether or not information constitutes personal data, please refer to the definition of personal data under separate guidance.

What is a valid Subject Access request?

A subject access request is a request from or on behalf of an individual (not a company) which seeks to discover whether you are processing the personal data of that individual (a data subject) and if so, to have access to that information.

Requests may be made informally so it is important to be able to recognise a subject access request as such when a request for information is made. A valid subject access request can be made in writing, either by letter, fax or email or verbally. It must be treated as a valid request regardless of how it is made.

Additional information may be required from the individual in order to process the request, as follows:

- Confirmation of identity – it must be established that the individual requesting the information is the person to whom the personal data relates
- Any information that is reasonably required to locate the personal data requested
-

All Subject Access Requests must be passed to the Managing Director in the first instance.

Guide to dealing with Subject Access Requests involving other people's information

When responding to a subject access request, there is a potential conflict between an individual's right of access and a third party's right to confidentiality.

Generally, if the third party information does not form part of the requested information, the names of the third parties may be redacted

However, if it is not possible to separate the third party information from that requested and if the response to a request will disclose information relating to a third party which may enable identification, the information does not have to be released unless:

- The third party has consented to disclosure; or
- It is reasonable in all the circumstances to comply with the request without the consent of the third party

Third party consent

Copyright ©
Produced by FT HR

There is no obligation to try and obtain consent and it may not be necessary in circumstances such as when the individual already knows the identity of the third party or where the third party is a health or social services professional.

Where it is difficult to obtain consent or where consent is refused, the issue of whether or not it is 'reasonable' to disclose the information must be considered.

Reasonableness

Regard must be given to the following:

- Any duty of confidentiality owed to the third party
- Any steps taken to obtain third party consent
- Whether the third party is capable of giving consent
- Any express refusal of consent by the third party

Duty of Confidentiality

This should not be assumed simply because a document is marked confidential.

Whether or not information is available to the public and has been disclosed with an expectation of confidentiality can help determine its existence. However, a clear duty of confidence exists between the following parties:

- Doctor/patient
- Employer/employee
- Solicitor/client
- Bank/customer
- Counsellor/client

If, for example, a reference for the individual was received from a doctor, it would be reasonable for this not to be disclosed. Likewise, if reference to the doctor is made in other documentation, this could be redacted prior to release.

A further example; if the third party information relates to an employee of the company who is not known to the individual it can be redacted. If the employee is already known to the individual, the information could be disclosed.

As there are no set rules regarding the issue of reasonableness each case must considered separately. Having considered the above, the potential impact of the release of such information must also be assessed and balanced against the individual's rights.

Finally, and as a general rule, if the information does not carry a duty of confidentiality and it refers to information received from a third party professional, such as a social worker, in their professional capacity, the information can be released.

*****An accurate record must be kept of any action taken together with the reasoning behind any decisions made as to why consent was not requested.*****

Guide to dealing with repeated/ unreasonable requests

Copyright ©
Produced by FT HR

Guidance from the Information Commissioner's Office provides that we are not obliged to comply with similar or identical requests to ones we have already dealt with unless a reasonable interval has elapsed.

Although no definition of reasonable is given, the following should be considered:

- The nature of the data – whether it is particularly sensitive
- Purpose of the processing – whether it could be detrimental to the individual
- How often the data is altered – whether or not the information is likely to have changed

If further data has been collected since the previous request the individual should be contacted and it should be agreed that only the new data will be supplied.

If no further data has been collected, the individual should be contacted in writing to explain why the data will not be supplied.

Exemptions

There are several exemptions to the provision of personal data, and the ones that are likely to apply are listed below:

- Confidential references given or to be given by the company relating to a person's education, training or employment
- Records of the intention of the company in relation to any negotiations with the individual to the extent to which the release of such information would be likely to prejudice those negotiations. This exemption would not apply after completion of the negotiations
- Personal data processed for the purposes of management forecasting/planning to assist the company in the conduct of any business. Again, only if the application of the subject access provisions would be likely to prejudice the company activity
- Information for which legal professional privilege (or its Scottish equivalent) applies

Further information for professionals dealing with subject access requests, and for individuals wishing to make such requests, is available on the Information Commissioner's Office website at http://www.ico.gov.uk/.

Copyright ©
Produced by FT HR