Bromford.

Information Governance Policy

1. Policy statement

Bromford protects our customers, colleagues, everyone we work with, and our business, by following good Information Governance principles, which make sure that all information (personal and commercial) is collected, stored, used, shared and disposed of safely and securely, in line with legal requirements and best practice. Our Information Governance Framework consists of this Policy and the linked reference documents.

2. Contents:

3. Legislative Requirements including links

Bromford's policy is to comply with:
Data Protection Act 1998
General Data Protection Regulation 2016 (enforceable from 25 May 2018)
Privacy & Electronic Communications Regulations 2003
Copyright Designs & Patent Act
Computer Misuse Act
Human Rights Act
Payment Card Industry: Data Security Standard (PCI-DSS)

Please note Bromford is not subject to the Freedom of Information Act 2000. For advice please contact the Governance Team.

Summary

What?

Information Governance is about making sure that all the information we come into contact with at Bromford – whether it's about people or about business matters – is handled properly throughout its "data journey". This means that all information must be collected, stored, used, shared and disposed of appropriately and securely, by following legal requirements and best practice.

The use of information about people, often described as 'personal data' or 'personal information', is specifically covered by the Data Protection Act 1998, which will be replaced by the General Data Protection Regulations in 2018. It can be information about customers, colleagues, or any other people Bromford has contact with.

Information Governance applies to all information, in any format, including hard copy and electronic copy, as well as photographs, videos, CCTV, telephone or sound recordings, not just written or typed information.

Why?

Information is a valuable asset, especially the personal information that our customers and colleagues entrust Bromford with, and we must handle it with respect and keep it secure. The consequences of an incident that results in personal or business information falling into the wrong hands can include serious harm and distress to individuals whose data is breached and harm to Bromford. Under Data Protection laws the business could be prosecuted and have large fines imposed, as well as suffer reputational damage.

Good Information Governance is an integral part of good customer service.

When?

The policy must be followed in all situations, including whether colleagues are working in the office, at home or at any other private or public location.

Who?

Everybody working at, and for, Bromford is responsible for good Information Governance. This policy applies to all colleagues, including permanent, temporary and fixed-term colleagues, contractors, consultants, people on work experience placements and Board and committee members and advisors.

How?

Colleagues can promote good Information Governance by:

- following this Policy, and other policies and How To guides linked to this this Policy and other IG communications;
- completing their Data Protection training;
- reporting suspected breaches to Governance and ICT;
- and querying anything that looks like poor Information Governance or that they are unsure of.

Leaders should:

- share this Policy and all policies and How To guides linked to this Policy, as well as other communications about IG matters, with their teams;
- make sure their teams complete their training;
- support their teams in reporting possible breaches;
- and design their policies and processes with good Information Governance principles in mind.

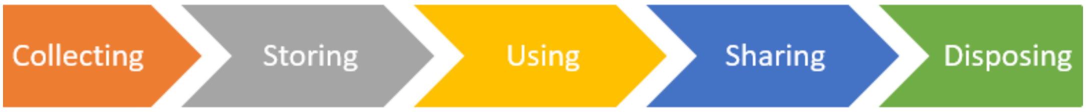
This policy contains a summary at the start of each section, and extra detail after each summary with references to useful, related documents. These documents are all hyperlinked from the front page of this policy.

The Quick Look Up section at the back of the policy contains definitions for some key terms sometimes used in Information Governance and Data Protection.

The Governance Team can provide extra help and advice.

The Information Journey

This diagram illustrates the stages that information goes through on its “journey” at Bromford, starting with when we collect it. Each stage carries its own risks and requires careful consideration.



Collecting Information

- We collect information in several ways, including when we:
    - use paper or electronic forms for people to fill in;
    - enter details into a computer or mobile device or paper files;
    - make written or typed notes;
    - receive or send emails, letters or phone calls, or
    - take photos, make videos or use CCTV.
- It includes when we receive information directly from the source or the person it’s about, or if we receive it from another person or organisation.
- A lot of the information is about people, so must be collected **fairly** and **lawfully.**
- This means it can only be collected for justified and specific reasons, and the amount collected **must not be excessive**.
- Information about people must not be collected ‘just in case’ we need it.
- The people the information is about **must be told clearly** why we are collecting their information, how we will use it, and who we will share it with, and sometimes they must give us their **consent** for the collecting and processing of their information.

Before we collect personal information:

Privacy Impact Assessments (PIAs) identify risks whenever we plan to collect, use or share personal information as part of a project, or when we plan to change the way we handle personal information. A PIA helps assess the severity of the risks, decide how they should be managed and put processes in place to control them. See the PIA How To and Template.

How we collect personal information:

Forms should be designed to only collect the minimum amount of information we need, and include a DP statement if collecting personal information (see the section on DP Statements below.) Doing a PIA can help when designing forms and processes.

Notes in writing or systems, or emails should always be factual and only include the minimum needed. The person/people being written about have a right to access the notes/emails, so they should be written with respect, with this in mind.

How we tell people about collecting their information:

Bromford's Privacy Notice is on our website. It explains how we process personal information; the way we collect it, how we use our records and what rights people have in relation to their own information.

Our Data Protection Statement for Forms explains how information will be used and should be included on all forms that are used to collect personal information. There is an extra section which should be used in the DP Statement if sensitive personal information is being collected.

Reasons for collecting personal information:

Most of the information we collect and hold is to allow us to provide a service to our customers, or to interact with other people, such as people making enquiries or complaints. This includes information that our contractors need to be able to provide a service on our behalf.

There may be times when laws and regulations require us to hold information about our customers or other people.

Sometimes we collect and hold additional information that is not strictly necessary in order to provide a service, but can help us to analyse and improve our services, such as Equality and Diversity information. When asking people these kinds of questions they must be made aware it is optional and feel free to not provide the information if they do not consent. It must be clearly explained why we would like to collect the information. The consent given must meet the criteria set out in the 'Definitions' section below.

If colleagues have any doubts or questions about the reasons we are collecting information, or about what we can do with information we plan to collect or are already collecting, they should speak to the Governance Team first.

Some specific types of information collecting:

Most information we hold is written or typed words, but it also includes other formats, some of which must be collected following special rules:

Taking card payments for services is done in line with the Payment Card Industry Data Security Standard (PCI-DSS).

Incoming and outgoing phone calls made via our main customer contact lines are recorded, and the recordings are 'personal information'. See the Recording Customer Calls How To.

CCTV use involves collecting, processing and storing images of people, which is 'personal information'. Any business area using CCTV must comply with all relevant legislation which governs the use and purpose of CCTV. See the CCTV Systems Policy and How To.

Photos, films and news stories are all 'personal information' and we must get permission from the people featured. Permission can be verbal, but we use a permission form if we want to use the photo, film or story for external publication. See the Permission form and guidance on the Comms Team area of OurSpace.

Storing Information

- Information, about people or the business, should not be kept any longer than we need it for the purpose it was originally collected.
- Sending it to offsite archive still counts as Bromford 'storing' the information.
- It should always be stored securely.
- See the section on Using Information for more on security.

Standard Business documents
So that our information for colleagues is clear, we use standard templates for Policies, 'How To' guides and reports. The latest versions are stored on Sharepoint/OurSpace.

Document and Information Retention / Archiving
Bromford's Document Retention Table sets out the length of time we can and should keep documents. You should refer to this before destroying or archiving documents.
Facilities Management provide secure archiving, through an external contractor.
Emails contain personal and business information and so should be regularly reviewed and deleted.

Facilities Management provide appropriate physical, technical, procedural and environmental controls to the main server site, such as access control, redundant air conditioning and power supplies, and temperature monitoring.

The server "back up" site is situated far enough away so as to not be affected by a potential disaster affecting the main site. The data is stored in an encrypted format on enterprise grade redundant storage.

Storing personal data outside the EEA:

The Data Protection Act places special restrictions around transferring personal information outside of the European Economic Area (EEA). "Transfer" includes storing personal information on servers outside the EEA, which is the most likely way Bromford information would be transferred outside of the EEA.

All Bromford core ICT services are located **within the EU**.

When we are working/contracting with a third party, who will then become a **Data Processor** for Bromford (e.g. IT contractors, sub-contractors etc.), the contract must include our standard Data Protection contract clause, which includes reference to the fact that data cannot be transferred outside of the EEA without prior written consent from Bromford.

Keeping info secure, but also available:

Keys to drawers and cabinets – keys must be made available at all times during working hours, including when colleagues are absent or on leave. This includes access to any electronic folders or documents that may be password protected.

Using Information

- Personal information can only be used for the purpose it was collected.
- If we think that information we've previously collected for one purpose (such as providing a tenancy) would be useful for another purpose we must make sure that we have a legal basis for using the information for the new purpose.
- This assessment should be done using a **Privacy Impact Assessment** (PIA - see the section above).
- All information should be kept up to date, and accurate, as much as possible.
- The use of systems that hold information is controlled and unacceptable use is not tolerated.
- We can only use information we have a legal right to, taking into account copyright and patents.
- While we are using information we must also keep it **secure.**

Information Quality:

All colleagues are responsible for the quality and accuracy of the information they handle and produce so they, and their leaders, must make sure they are familiar with relevant processes and procedures. If colleagues are unsure about their work and the information they are handling they should speak to their line manager. If we're made aware that personal information is out of date or inaccurate it should be amended as soon as we are made aware, or deleted is appropriate.

Teams who work directly with customers should check that customers' personal details are up to date and accurate as often as possible.

Periodically, colleagues are asked to check and update their own personal details on the HR system.

Copyright and Patents - Colleagues are responsible for making sure they are aware of any copyright or patent that may apply to any software and/or information (e.g. graphics, files, documents, messages) they want to use and must not copy any information or materials that are protected by copyright/patents.

Access to information/systems:

Colleague Access
Through the starters process colleagues will be provided with the relevant level of access to the network, systems and information.
When ICT are notified of a leaver, user accounts will be managed following the Leaver and absence management process. If appropriate, email accounts will be linked to that of an authorised colleague to have access to the leaver's mailbox, for a limited time.

Password Management
Secure passwords are essential. Please see the ICT Acceptable Use Policy, for more details on "secure" passwords and the Do's and Don'ts of Password Management. Generic passwords should not be used and passwords should not be shared.

Unacceptable use of Information/systems/equipment:

Bromford equipment must only be used in line with this policy, and not used for any illegal activity. Any information colleagues come into contact with during their work must only be used for their work.
Any colleague breaching this policy will go through disciplinary procedures.
Any illegal activity will be viewed as gross misconduct and, where appropriate, will be reported to the Police. Such illegal activities include, amongst others:

- Stalking;
- Hacking;
- Fraud
- Drug misuse (includes drug dealing);
- Paedophilia;
- Terrorism;
- Incitement to racial harassment or violence;
- Cyber bullying / harassment or victimisation;
- Any misuse of someone else's personal information.

It is a **criminal offence** for any colleague to misuse or disclose **personal information** that they have access to for their work, or to purposefully gain access to personal information that they do not need for their work.

Using equipment, software & services that store information:

Equipment & Software
Bromford-owned equipment (e.g. iPads, PCs, laptops, printers, network equipment, phones and software) are provided to colleagues to help carry out their job effectively and efficiently.
Use of additional equipment that stores data, such as USB sticks, is restricted.

Only licenced software (including downloads) should be installed on Bromford's equipment and the installation must be installed by ICT. Colleagues/teams that want a new piece of software (including cloud hosted software) must request it from ICT, who will consider requests.

Public Wi-Fi

Security features on Bromford-owned laptops/tablets reduce the risks when using public Wi-Fi connections, but colleagues should avoid using other devices to connect to Bromford services via public Wi-Fi if possible, and be aware of the risks if connecting their own devices to the internet via public Wi-Fi. Most Wi-Fi made available by large, established companies can be expected to have good standards of security, but this might not be the case everywhere.

ICT Systems Development & Maintenance

The Senior ICT Management team will ensure that any internal system development activities operate within required legislation and industry standards.

All information systems being tested (whether new or existing) are isolated from “live” information systems during the testing period. We will use randomised data or an offline copy of a live data source to perform testing and UAT activities ahead of a change. Any third party system development and testing is done in line with relevant legislation and industry standards.

Change Management

Standardised methods and procedures are in place for efficient and prompt handling of all ICT system changes, to minimise the number and impact of any related incidents upon service. See the Change Management Policy.

Patch Management

All patches relevant to Bromford’s infrastructure services systems (e.g. laptops, ActiveH, Windows, servers, etc.) are applied by ICT or approved third party suppliers, either on a needs basis or at regular scheduled intervals. Colleagues should regularly connect their devices to the internet or network to receive all relevant patches and updates in a timely fashion. This helps to protect our devices and network.

Use of Email/instant messaging & Internet including social media:

All colleagues are responsible for making sure they have read and understood the ICT Acceptable Use Policy, and must comply with it.

External email and internet access is usually given to everyone and colleagues are asked to take care when using email, messaging, and social media. Personal use of our systems is a matter of trust between Bromford and colleagues. Personal use must not interfere with the day to day work of the business, must not cost the business anything, and must not breach any policies or regulations.

Access to some sites is blocked and some emails may be quarantined. Colleague use of email and the internet is logged and can be monitored, but Bromford doesn’t normally access these logs or the content of emails unless there are reasonable grounds for doing so.

Sending Email - Emails sent to other organisations are formal communications from Bromford, so should be treated with the same care as a letter, for example. A standard notice is electronically added to outgoing emails, which includes our contact details and states that the email is confidential, and contains a link to the full Email disclaimer on our website.

Receiving Emails- Colleagues need to be aware of phishing emails. This is a fraudulent email asking you to confirm details or click on a link: colleagues should **never respond** to these requests or click on links from unfamiliar or **suspicious emails**. Any suspicious emails should be reported to the ICT Helpdesk.

Use of Social Media is encouraged, but you should consider time spent on personal social networking similar to taking personal phone calls at work.
Social media posts on behalf of Bromford should be treated with the same care as any other communication, such as a letter or email. See the guidance on the Comms Team Our Space pages.

Physical security – Business responsibilities:

Facilities Management look after building security at our main offices, including making sure building entrances and car parks are secure, especially when the offices are closed, security doors are working and the visitor procedure is in place.

Visitors - Facilities Management/People Services look after visitors to our main offices, including announcing visitors at Reception, managing parking and giving out visitor passes.

Colleague badges and passes - Facilities Management /People Services give all colleagues identity name badges and at our main offices give out car parking passes, and security passes.

Printers/photocopiers at main offices are operated by inputting an individual PIN code, so only authorised colleagues can print or photocopy.

Physical Security – Colleague responsibilities:

Visitors must be supervised by a Bromford colleague, but not necessarily accompanied at all times.

Identity badges and passes - All colleagues have an identity badge, which should be worn at all times, and a security passes (to move around the building) which must be kept secure and not given to anyone unauthorised.

Portable ICT equipment including laptops, phones and iPads should not be left unattended in a public place when working offsite, and should not be left overnight in a car/van. They should be kept secure either at home or in the office, as far as is practical.

Locked screens - Colleagues must make sure their screens are locked if equipment is left unattended for any period of time, even if they are still in the office and getting a drink, for example.

Clear desks - All colleagues are responsible, at all times, for making sure desks and any other working spaces, such as break-out areas, are kept tidy. Nothing should be left out for anyone passing to be able to pick and look at. Colleagues are encouraged to work in a paperless way but any paper-based personal or commercially sensitive information or files should be in locked cabinets when not in use.

Mobile working – Colleagues must take special care when working outside of the office, at home or in another location, to keep information secure. Remember:

- Keep your devices secure, especially overnight (not in a vehicle);
- Think about where you keep your paperwork just as much as your devices;
- Be aware of where you're having conversations, and who can hear you;
- Be aware of who can see your screen or paperwork;
- If you're working remotely or with a customer, every time you leave a location take a minute to check you have all your papers and devices with you, so you don't leave anything behind
- If your device or any paperwork does get mislaid or stolen, please report it to ICT & the Governance Team as soon as possible so we can protect our data.

Sharing Information

- Sharing any type of information – business or personal information – is high risk, and must always be approached with care
- Even internally, sharing should always be on a need to know basis.
- Sharing must always be legal and it must always be done securely, so that it isn't lost or accessed by the wrong people.
- If it is information about people, to be legally shared, it must be justified under the Data Protection Act.
- See the 'Sharing Personal Information – How To' (and the related 'Information Sharing Request Form'), and the 'Send & Share Information Safely & Securely - How To'.
- The people whose information Bromford holds have the legal right to receive copies from us of that information, known as making a Subject Access Request (SAR.)

Colleague contracts
Forming part of all colleagues' employment contracts terms and conditions is an agreement to maintain the confidentiality of all of Bromford's confidential information assets.

Casual colleagues (including contractors, agency etc.) will be required to agree and sign a Confidentiality Agreement prior to access being given to any of Bromford's information assets.

Colleague Shared Working

Information about people, or commercially sensitive information, must only be shared on a strict need to know basis, even amongst Bromford colleagues. And any legitimate sharing must be done securely, by following the 'Send & Share Information Safely & Securely - How To', and using the available tools, for example encryption when sending a document to a colleague by email.

The Scratch Drive can be accessed by all Bromford colleagues and should not be used for storing any information for any length of time. If you need to share a large file with a colleague, save it to the Scratch Drive at a time when you know they can pick it up straightaway, then delete it.

For continued shared working between teams, use a Shared Working Area on OurSpace, which can be requested by emailing the Helpdesk.

Working with contractors/processors
Whenever we are entering into a contract where the third-party will be a '**Data Processor'** the contract as a whole should be reviewed for appropriate Data Protection/Information Governance controls, and if appropriate, a PIA completed. This includes where:

- the contract involves **sharing** personal information (about our customers, colleagues or anyone else) with a third-party, such as a partner, supplier or contractor; or
- a third-party will **store** personal information we give them on their computer systems, servers or at their premises (this includes archiving.)

In addition, there must be a **Data Protection clause** in the contract.
See the DP Clauses in Contracts – How To.
See the PIA How To.

Working with partners - ISAs
Sometimes when we are working with partner organisations, such as Local Authorities, we sign up to an Information Sharing Agreement ('ISA'), also sometimes known as an Information Sharing Protocol. We do not have to be signed up to an ISA in order to share information (either giving it or receiving it) and just because we have an ISA with an organisation does **not** mean we automatically **have** to share any information with them. We must only share personal information when we're satisfied that the sharing is **fair and legal**. See the Using Information Sharing Agreements (ISAs) – How To

Social Media, incl. Yammer

Colleagues must be very careful to not accidentally disclose commercially confidential information or other people's personal information in social media posts. This includes using Yammer, which must be treated with the same care as other social media. Customer details should not be shared, even if colleagues are sharing a thank you from a customer, or a good news story, unless they have agreed to be part of an official Comms Team led story. Guidance is available on Ourspace about using Social Media.

Subject Access Requests

A Subject Access Request (SAR) is the legal right of people to ask Bromford for copies of all the information we hold about them.

It is our policy to be as open and transparent as possible, and to give people copies of their own information, and things like letters that have previously been sent to them, if possible, without them having to make a full Subject Access Request.

The Governance Team look after SARs and can help with any colleague or customer queries. See the SAR Information Page on Our Space.

Disposing

- All personal and business information must be disposed of securely, so that it can't be found or accessed later, and possibly misused or seen by the wrong people.
- Personal information must be disposed of when it is no longer needed for the reason it was collected.
- Use the confidential disposal bins or shred any paper copies and seek advice from ICT about how to permanently dispose of any information held electronically.
- See the Document Retention Table for advice on when to dispose of information and documents.
- Archiving is not the same as disposing of information or documents. Archived documents should be called back and securely destroyed at the end of their retention period.

Hard copy information

Facilities Management provide secure recycling bins, through an external contractor, at the main offices for hard copy information to be shredded.

ICT equipment

ICT manage the disposal of all ICT equipment, this will include the disposal of kit that may contain personal data and confidential information on hard drives in PC's and laptops and servers, back up tapes, mobile phones and tablets.

The disposal process ensures that all devices sent for disposal are recorded by serial number/asset tag or for mobile phones imei numbers. Disposal kit is securely stored (until disposal collection) and securely transported and stored with the disposal contactor. Hard drives that may contain data are securely destroyed to industry standards within 5 working days.

Following each disposal, ICT ensure the correct waste transfer paperwork is supplied, in line with the WEEE regulations and where necessary, appropriate data destruction certificates are issued.

Handling IG Incidents

- Losing personal information could cause harm or embarrassment to the people the information is about.
- It could also lead to Bromford being prosecuted and fined (currently up to £500,000) and we could suffer serious reputational damage.
- Losing business information could cause harm to Bromford in various ways.
- Any loss or suspected loss of personal or business information – whatever the reason – must be reported as soon as possible to both the Governance Team and ICT Team as explained below.

Lost / stolen devices

All colleagues should report any loss or theft of ICT equipment to the ICT Team as soon as possible. ICT will take appropriate and swift action to track and disable/wipe the device if this is possible.

Data loss

Any loss, or suspected loss, of personal or sensitive business information, must be reported as soon as possible – either directly to the Governance Team or to the ICT Team who will report to the Governance Team. The Governance Team can help to mitigate the risks, investigate what happened and assess the breach against the data protection regulator (Information Commissioner’s Office) reporting guidance. Colleagues should take any appropriate actions to attempt to recover the information first; for example, attempt to recall an email sent in error.
See the Handling DP Issues & Breaches – How To.

Managing cyber attacks

All cyber security incidents will be assessed, managed, logged and reviewed by the ICT Team, who will work to recover any lost information and mitigate risks. The Governance team will be involved for reporting any attempted or successful fraud or any Data Protection breaches.
See the Cyber Security Policy/Cyber Incident Response Plan.

Disaster Recovery & Business Continuity

The ICT team make sure processes are in place to protect our data and provide continuity of access to our data if an incident occurs that causes disruption to the business.
Events may include, amongst others:

- Infrastructure / system failure

- Fire, flood, impact damage
- Power disruption / failure
- Malicious (Hacking) attack
- Theft of information / media

See the Major Incident Plan, Disaster Recovery Plan and Business Continuity Plan documents.

Monitoring and Review

Risk Management monitoring
Bromford's Risk Management framework involves identifying risks at a number of stages, including business planning, in key projects and in day to day business. Controls and assurances are designed to prevent risks from materialising as far as possible. Key risks are monitored and reported to the Executive Board and Assurance & Audit Committee.

Training monitoring
Training is monitored by the Learning and Development team identify and communicate with those colleagues that have not completed required training.

Systems monitoring
Monitoring is in place on all information systems to detect any unauthorised activity (e.g. external or internal attacks) or security breaches (e.g. as a result of penetrating Bromford's network a third party has managed to access and remove certain information assets).

If any suspected security incidents or breaches are identified by ICT, the Cyber Attack plan will be followed.

Content monitoring
Bromford reserve the right to analyse all content from the monitoring logs/records of all activity pertaining to both equipment (i.e hardware) and software, including Internet & Email usage at any time for:

- Performance management
- Fault diagnostics
- Audit requirements
- Unauthorised & Unacceptable use of IT systems; software and equipment

Policy approval and Review
This policy has been approved by the Executive Board, who will review it every three years. The Head of Governance will review compliance with this policy on an annual basis and, if necessary, report (with recommendations) to the Executive Board.
Amendments to this policy may be approved by the Head of Governance.

Quick look up

Glossary of terms used in Information Governance and Data Protection:

DPA	• Data Protection Act 1998 - the current UK DP regulations.
GDPR	• General Data Protection Regulations – due to replace the DPA in May 2018.
Personal Information	• **Any** information that can **identify** a living person, either on its own or **with other** information. It does not need to include a person's name. • Includes **comments or opinions** about a person. • Including; information held on computer systems, in paper files, in emails, photographs, CCTV footage, on social media.
Sensitive personal information	• Anything about a person's ethnic origin, political opinions, religious beliefs, memberships of trade unions, physical or mental health, sexual life, or criminal offences (alleged or committed). • Must be treated with extra care, in line with **specific rules** in the DPA about sensitive data.
Data Subject	• The person that the information is **about**.
Data Controller	• A person or organisation with the authority to decide how and why personal information is used. • Bromford's 'Data Controllers' are **the legal entities** – Bromford Housing Group, Bromford Housing Association, Bromford Home Ownership, and Bromford Developments – and are **registered** with the Information Commissioner's Office ('ICO') as required. • The registration numbers and renewal dates are on our **website**.
Data Processor	• A 3rd party person or organisation which **processes** personal data **on behalf** of a Data Controller. E.g. service providers, contractors and hosts for IT systems. • Bromford colleagues are **not** considered Data Processors.
Processing	• Processing covers **anything** that can be done to information. • This includes; collecting, recording, storing, using, amending, sharing, disposing of or destroying personal information.
Consent	• Permission from the data subject to collect and process their information. • It must be **clear** and **unambiguous**. • We must not ask for consent if we can and would process the information anyway unless we are prepared to accept the consent later being withdrawn. (Cont. over)

	• Cannot be hidden in the terms and conditions or contract clauses. • Consent obtained from someone who does not feel they are able to refuse consent is not valid.