



## BOARDING BRIEFING PAPER

### NUMBER SIXTEEN

JANUARY 2005

## THE DATA PROTECTION ACT 1998 Implications for Boarding Schools

prepared by

**Farrer and Co.  
Solicitors  
66 Lincoln's Inn Fields  
London WC2A 3LH**

THE BSA GRATEFULLY ACKNOWLEDGES THE SUPPORT OF THE

department for

**education and skills**

creating opportunity, releasing potential, achieving excellence

**FOR THIS PUBLICATION**

The Boarding Schools' Association  
Grosvenor Gardens House  
35-37, Grosvenor Gardens, London SW1W 0BS  
Tel : 020 7798 1580 Fax : 020 7798 1581  
e-mail : [bsa@boarding.org.uk](mailto:bsa@boarding.org.uk)  
Website: [www.boarding.org.uk](http://www.boarding.org.uk)

## 1. The 1998 Act: an Introduction

The Courts have described the 1998 Act as “*a thicket*”. The latest campaign, however, from the Information Commissioner (responsible for regulating the workings of the 1998 Act on a day-to-day basis - see below for his contact details) is entitled “*Make Data Protection simpler*”. The 1998 Act is, in general terms, designed to balance the privacy rights of individuals on the one hand against the legitimate interests of organisations using their personal data as part of their business activities on the other. Before considering how the 1998 Act affects boarding schools, however, it is important to understand certain key terminology.

## 2. The 1998 Act: Key Terminology

- Personal Data

The 1998 Act governs the “*Processing*” (see below) of “*Personal Data*”. Personal Data is defined as any data relating to an identifiable living individual, whether processed by computer or (with certain exceptions) in paper-based filing systems. Significantly, the definition includes expressions of opinion and intention about “*Data Subjects*” (see below) and the definition can include photographs and images, for example, material contained on a school website or in promotional literature.

In a recent case before the Court of Appeal, *Durant -v- FSA*, the Court applied a narrow definition to the type of information which will constitute Personal Data and which is governed by the 1998 Act. Previously, it was thought that any information howsoever relating to a particular individual would probably constitute Personal Data. Post-*Durant*, however, the 1998 Act will only apply to information which affects an individual’s privacy, whether in his personal or family life, business or professional capacity. The concept of privacy is central to the definition of Personal Data and the degree to which the processing of information might have an adverse impact on an individual is something to be taken into account.

The Court indicated that when considering whether or not the information in question affects an individual’s privacy, the question of whether the information is biographical in a significant sense is important. The information will have to go beyond the mere recording of an individual’s involvement in a particular matter or event where this has no personal connotations before it will constitute Personal Data.

The Court said that for information to constitute Personal Data it must have the particular individual as its focus, rather than some other person with whom he may have been involved or some other transaction or event in which he may have featured or had an interest. Simply because an individual’s name appears on a document, the information contained in that document will not necessarily be Personal Data about the named individual. For example, incidental mention in the minutes of a meeting of an individual’s attendance is unlikely to constitute Personal Data. Similarly, where an individual’s name appears on a document or e-mail indicating only that it has been sent or copied to that individual, again the contents of that document or e-mail are unlikely to constitute Personal Data.

- Data Subjects

Data Subjects are the living individuals with rights under the 1998 Act. The 1998 Act does not contain any provision as to the minimum age of a Data Subject. Guidance from the Information Commissioner indicates that, provided pupils are able to understand their rights in broad terms, then it is they (and not their parents or guardians) who will be treated as Data Subjects. Where pupils are incapable of understanding their rights or of understanding the consequences of the 1998 Act, then the Information Commissioner advises schools to deal with parents or guardians in the usual way. As pupils are unlikely to have an in-depth and precise legal understanding of the 1998 Act, however, it is likely that the Information Commissioner would apply a relatively low threshold so as to consider most pupils as Data Subjects more often than not.

- Data Processing

The 1998 Act governs the processing of Personal Data. The definition of processing is wide. It covers almost any activity involving Personal Data, including obtaining, recording, holding, consulting, using, altering, disclosing, sharing and even destroying Personal Data.

- Data Controllers and Data Processors

The 1998 Act regulates the activities of those responsible for determining why and how Personal Data is processed. Such entities are defined as “*Data Controllers*” and in the schools sector, the Headmaster and Board of Governors (those that take ultimate responsibility for decision-making) would be considered a Data Controller although, of course, in the usual way, day-to-day responsibility can be

(4)

delegated. It is commonplace for the Bursar, for example, to take responsibility for data protection issues. Although the 1998 Act includes certain criminal offences (see below), a director, manager, secretary or other similar officer of a corporate body will only be liable for the same offence as proved against that corporate body where there has been connivance or neglect by that officer.

Where a Data Controller (such as a school) contractually engages a third party to carry out Data Processing on its behalf (such as alumni mailing or record management or destruction), then the 1998 Act defines the third party as a “*Data Processor*”. In these circumstances, the contractual arrangements must be in writing and must include a provision by which the Data Processor agrees only to act on the instructions of the Data Controller and to ensure appropriate technological and organisational measures are taken so that the Personal Data in question is kept properly secure.

- Sensitive Personal Data

The 1998 Act governs certain types of Personal Data, defined as “*Sensitive Personal Data*” in a more restrictive way. The specific categories of Sensitive Personal Data are data consisting of information as to a Data Subject’s:

- race or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- commission or alleged commission of any offence; and
- proceedings for any offence committed or alleged to have been committed.

The above list is exhaustive. For example, details of a Data Subject’s wealth or career are not “*sensitive*”. The way in which the 1998 Act imposes additional compliance requirements on Data Controllers so far as Sensitive Personal Data is concerned is explained below.

- Relevant Filing Systems

Earlier legislation only regulated Personal Data being processed by computer or other automatic means. The 1998 Act, however, extends this definition to include both computer/automated processed Personal Data and (with certain exceptions) paper-based filing systems and other non-electronic collections of Personal Data. Where Personal Data is stored in paper form, it will only be governed by the 1998 Act where it is contained within a “*Relevant Filing System*”. This definition has no relevance to Personal Data processed electronically or by computer. The key characteristic of a Relevant Filing System (so far as paper-based records are concerned) is the requirement for structure and ready accessibility of specific information.

In the *Durant* case, the Court of Appeal recognised the difficulties faced by Data Controllers where the 1998 Act is to apply to paper-based records and it adopted a restrictive interpretation of what types of paper records would fall within the definition of a Relevant Filing System and would thereby be caught by the Act. Effectively only paper-based records which are sufficiently sophisticated to allow for the same or similar ready accessibility of specific pieces of information (akin to a computerised filing system) will be governed by the 1998 Act. Anything less by way of sophisticated structure, for example a filing system of paper-based records which requires a searcher to leaf through files to see what and whether information qualifying as Personal Data is to be found there, would bear no resemblance to a computerised search and would therefore not qualify as a Relevant Filing System.

The Court held that if the 1998 Act was to have any sensible and practical effect, in the context of paper-based filing systems, it would only apply to a system which enabled the identification of specific pieces of information within the records with a minimum of time and costs, through clear referencing mechanisms to allow a searcher to go straight to particular information without having to flick through the entire file contents.

Even where information is filed in a system using an individual’s name as a file name, this may not qualify as a relevant filing system if the indexing/referencing/sub-division is not sufficiently sophisticated to avoid the need to leaf through the file itself to find particular pieces of information. Where files are structured purely in chronological order, it is more unlikely still that they will be

considered a Relevant Filing System where there is no appropriate structure or indexing in place. Some personnel files or other manual files may be sufficiently sophisticated in their structure to constitute a Relevant Filing System perhaps where there are clear sub-dividers (such as sickness, absence, contact details etc). However, the *Durant* decision means that it is likely that very few manual files will be covered by the provisions of the 1998 Act and most information held in paper-based records is unlikely to fall within the Data Protection regime.

### 3. The Data Protection Principles: Statutory (Good Practice) Requirements

Schools, as Data Controllers, must comply with eight Data Protection Principles contained in the 1998 Act. All aspects of a Data Controller's processing must be kept under regular review to ensure that the principles are complied with. The implications of some of the principles are self-evident. Others are more complex and require some explanation.

The Data Protection Principles require Personal Data always to be:

(i) Processed fairly and lawfully.

- The first principle which requires all Personal Data to be processed "*fairly and lawfully*" is a central element of the 1998 Act. To ensure compliance with the 1998 Act, a Data Controller must pass through one of six pre-conditions. These are known as the "*gateways*" to fair and lawful processing and are found in Schedule 2 of the 1998 Act. The most obvious gateway is where the Data Subject has consented to the processing in question. Such consent (so far as non-sensitive Personal Data is concerned) can either be explicit or implied. The 1998 Act also requires Data Subjects to be aware of the identity of the Data Controller (usually self-explanatory) and the purpose or purposes for which the data are intended to be processed and any other further information to ensure fairness. This means that pupils and parents (and employees or other data subjects about whom a school processes Personal Data) must be properly informed about the manner in which their information will be used by the school.
- The use of "*opt-in*" or "*opt-out*" boxes is now commonplace. It is not sufficient, however, for a Data Controller merely to give Data Subjects notice of its intention (say, to share Personal Data with third parties as part of some new commercial venture) and to assume consent (i.e. the "unless we hear from you to the contrary" approach). A failure to respond to a mail-shot in these terms should not be taken as a form of implied consent. Although "*opt-out*" boxes can be used to indicate consent, this will only be the case where the Data Subject has otherwise signified this position by some active and reciprocal communication between the parties. This means that if a school intends to use individuals' Personal Data for something not already consented to (or otherwise permitted - see below) and if it sends out a mail-shot of some description allowing individuals to opt-out, the school will only be permitted to use the Personal Data in this way if, as part of the exercise, a response is received back from the individuals which shows that they have had the opportunity to opt-out but have chosen not to do so (e.g. the "tear-off" slip is returned as part of some related communication booking).
- There are a number of other alternative gateways to fair and lawful processing (of non-sensitive Personal Data) in the absence of consent. For example, consent is not required where the processing is necessary for the performance of a contract with the Data Subject, which is helpful, of course, in the employment context. Processing is also fair and lawful (without consent) in order to protect the "*vital interests*" of the Data Subject, which would cover emergency situations where information about a Data Subject needs to be shared.
- A further alternative gateway, in the absence of consent, permits processing for the purposes of the "*legitimate interests*" of the Data Controller provided this is not unwarranted by reason of prejudice to the Data Subject. There is no definition of "*legitimate*" in the 1998 Act but this will generally include any processing necessary for a Data Controller's (such as a school's) day-to-day activities. This is a very useful alternative to obtaining consent when dealing with non-sensitive Personal Data.
- All of the above gateways apply to non-sensitive Personal Data. However, in the case of Sensitive Personal Data (see above for the categories of this sort of Personal Data) more restrictive rules apply. These are contained in Schedule 3 of the 1998 Act. In addition to passing through one of the above gateways from Schedule 2, Data Controllers must also pass through a second gateway from Schedule 3 before the processing of sensitive Personal Data will be fair and lawful and in compliance with the first principle.
- In the case of Sensitive Personal Data, any consent must be "*explicit*". Guidance from the Information Commissioner suggests that this requires a Data Subject to be given the specific detail of the processing concerned and the particular types of Sensitive Personal Data to be processed and for clear consent to be given. Explicit consent can thus be obtained by providing a comprehensive

notice of the intended purposes for Sensitive Personal Data processing, together with an opt-in tick box or signature box by which the Data Subject can indicate his consent.

- As with the gateways for non-sensitive Personal Data, there are a number of other helpful alternatives where explicit consent has not been obtained in order to process Sensitive Personal Data lawfully. For example, Sensitive Personal Data may be processed to comply with employment law obligations. There is also a similar “vital interests” gateway for processing Sensitive Personal Data which includes processing of an individual’s Sensitive Personal Data to protect the vital interests of him or another person. This again would be useful so far as health data is concerned where, say, a pupil is unconscious or cannot be found. Any Sensitive Personal Data deliberately made public by the Data Subject can be processed without consent as can processing of an individual’s Sensitive Personal Data where necessary in connection with legal (or prospective) legal proceedings or the obtaining of legal advice. In similar fashion to the “vital interest” gateway Sensitive Personal Data can also be processed without consent for medical purposes where the processing is carried out by a medical professional or somebody who owes a similar duty of confidentiality. Other gateways include processing in relation to unlawful activity and also processing in the public interest in relation to confidential counselling.
- Care should always be taken to ensure that all processing or potential processing of Personal Data (and Sensitive Personal Data) is fair and lawful. Processing of Sensitive Personal Data must comply with a pre-condition from Schedule 3 (as above) and one from Schedule 2. Processing of non-sensitive Personal Data need only comply with one of the pre-conditions from Schedule 2. Only then, in addition to ensuring that Data Subjects are fully informed as to the nature of any ongoing processing, will a Data Controller be acting fairly and lawfully and in compliance with the 1998 Act.
  - (ii) Obtained for specified purposes and only processed in accordance with those purposes.
  - (iii) Adequate, relevant and not excessive.
  - (iv) Accurate and, where necessary, kept up-to-date.
  - (v) Kept only for so long as is necessary for the specified purposes.
    - The Act does not specify any timeframe for the disposal of Personal Data. The law of contract and negligence allows claims to be brought within six years. Certain employment records, particularly health and safety issues, are required to be kept for longer periods. Schools should not, therefore, alter their usual record retention policy out of concern for the 1998 Act provided such policies or procedures reflect an appropriate approach to keeping material on file as well as maintaining a proper historic record of the school and those who work and study there.
  - (vi) Processed in accordance with Data Subject rights.
    - The rights of Data Subjects are explained in more detail below.
  - (vii) Kept secure.
    - The 1998 Act requires Data Controllers to adopt appropriate technical and organisational measures to avoid unauthorised or unlawful processing of Personal Data and to avoid accidental loss or destruction or damage to it. Put simply, schools ought to treat Personal Data, so far as security is concerned, in a way commensurate with the nature of the data in question. For example, pupils’ health records should be kept properly secure and it is likely that any existing common-sense approach to such matters would be Act-compliant.
  - (viii) Transferred outside the EEA only when the country in question ensures adequate legal protection for Data Subjects.
    - The ban on transferring Personal Data outside the EEA is not absolute and there are circumstances in which transfers are permitted. Schools may well wish to transfer Personal Data outside the EEA, for example to overseas alumni groups. Any Personal Data contained on a school website will automatically fall to be dealt with in the light of this principle because the world-wide web constitutes a world-wide transfer of Personal Data. Certain countries outside the EEA have been deemed “*safe*” by the Information Commissioner. Otherwise the Data Controller may make a decision about the adequacy of local legal protection in such countries.
    - The eighth principle includes nine circumstances in which the transfer ban outside the EEA will not apply. These circumstances include the Data Subject having consented to the transfer; the transfer being necessary for the performance of a contract between the Data Controller and the Data Subject and the transfer being necessary to protect the vital interests of the Data Subject. As with

the first principle, informed consent is a useful means by which schools can ensure that any transfers of Personal Data outside the EEA are lawful.

#### 4. Data Subject rights

Data Subjects (see above for advice on the standing of pupils as Data Subjects) have a number of rights expressly provided for in the 1998 Act. These rights include:

##### 4.1 Subject access

Data Subjects have a right to ask Data Controllers for access to Personal Data being processed about them held either in paper-based records (as caught by the 1998 Act post-*Durant*) or electronically. Requests ought to be made in writing and a maximum fee of £10 can be charged. Data Controllers must comply with such requests within a 40-day time period.

However, in making such a request for access, the comments of the Court in *Durant* have to be borne in mind. Requests can only be made for information which constitutes Personal Data (information which is biographical in a significant sense) and where paper-based records are concerned, requests for access only apply to Relevant Filing Systems (i.e. systems which are sufficiently sophisticated and well-structured).

There are also a number of exemptions with relevance to the schools sector. For example, references given or to be given by a school in relation to education or employment are exempt from subject access rights as are Personal Data processed by way of management planning or forecasting. Anything written down by candidates in examinations which constitutes Personal Data is exempt from subject access and the 1998 Act modifies the time limits for compliance with a subject access request where the Personal Data consists of examination results. Records which, if disclosed, might harm the physical or mental health of the data subject or any other person and any record indicating any risk of child abuse are exempt from subject access as are data concerning obtaining legal advice or subject to legal professional privileges. Personal Data processed as part of household or domestic activity is also exempt from the Act and so individuals' telephone books or Christmas card lists will not be caught, provided such processing is for non-commercial and domestic purposes only.

##### 4.2 Processing likely to cause damage or distress

Individuals can give notice in writing to Data Controllers requiring them to cease or not to begin processing which causes or is likely to cause unwarranted and substantial damage or distress to the Data Subject or to another person.

##### 4.3 No processing for direct marketing and no automated decision taking

Individuals can give notice in writing to a Data Controller to cease or not to begin any processing by way of direct marketing and similarly notice can be given to prevent a Data Controller from taking decisions that "*significantly affect*" a Data Subject where such decisions are taken solely by automated means.

##### 4.4 Rectification, blocking, erasure and destruction

The 1998 Act also allows Data Subjects to apply to the Court for an order requiring a Data Controller to rectify, block, erase or destroy Personal Data (including opinions) which are "*incorrect or misleading as to any matter of fact*".

##### 4.5 Compensation

The 1998 Act does provide for civil claims for compensation for breach of its terms. However, compensation will only be available where a Data Subject suffers financial damage (and distress) as a result of a breach. Compensation for distress alone is only available where the breach arises as a result of journalistic, literary or artistic activity. There is a defence for Data Controllers to show that they took reasonable care in attempting to comply with the Act.

#### 5. Notification

All Data Controllers are required to notify their activities to the Information Commissioner, details of which are included on a public register available on-line through the Information Commissioner's website. Failure to notify the Information Commissioner of processing undertaken by a Data Controller is a criminal offence. Notification is achieved by way of a standard form and in return for a fixed fee (£35). The Information Commissioner has prepared a standard template form for the schools sector. The entry on the notification register is to be renewed annually and the Information Commissioner sends out a reminder.

Recently, a number of organisations have begun to offer “*Data Protection Registration*” services. Such scams use official-looking headed notepaper and include threatening legal language. Excessive fees are charged by such companies who undertake to notify the Information Commissioner on behalf of Data Controllers. Schools ought, therefore, to be on their guard against such bogus notification/registration agencies.

## 6. Conclusions

The 1998 Act is a complicated area of the law which imposes broad and descriptive obligations on schools as Data Controllers with little guidance as how best to interpret concepts such as “*fair and lawful*”. However, the Information Commissioner is determined to ensure that the 1998 Act is applied in a sensible and pragmatic way and the Courts have followed suit. The provisions of the 1998 Act ought not to interfere with good governance and appropriate data management so far as the schools sector is concerned. Nevertheless, the 1998 Act imposes an additional layer of regulation about which those responsible for legal compliance ought to be aware.

## 7. Two further points

1. Paper records in the form of **internal memos** can contain personal data or sensitive personal data, just as emails might. However, what will be of importance is how they are filed away. If the internal memos form part of a “relevant filing system” then, if they contain personal data, then that personal data will be subject to the Act (taking account of course of the various exemptions and so on).

If however, these memos are not stored within a relevant filing system when they are filed away (most probable if they are filed chronologically or without any internal structuring or indexing), then the information contained in the memos (as part of manual paper-based records) is more likely to fall outside the scope of the Act altogether.

2. The Act regulates the **destruction or deletion of records** (paper or electronic) to ensure that this is done carefully to avoid any unwitting disclosure of personal data to third parties. Furthermore, the Act says that personal data should not be kept for longer than is necessary. This does not mean that schools should rush to delete their very useful databases. Firstly, there will always be a minimum amount of data needed to maintain an historic and informed record of pupils passing through the school. Also, the law in other areas (employment law; contract and tort litigation; health records) might give rise to recommended or mandatory periods of retention. For example, contract claims can be brought up to 6 years after an alleged breach. A common sense approach should be adopted.

## 8. Useful contacts and sources of information

The Office of the Information Commissioner  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire SK9 5AF

Tel: 01625 545700

[www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)

Farrer & Co  
Solicitors  
66 Lincoln’s Inn Fields  
London WC2A 3LH

Tel: 020 7242 2022 (Ref: JAP/BRB)

[www.farrer.co.uk](http://www.farrer.co.uk)

### Summary of Key Points

The Act applies to Personal Data relating to living individuals. These individuals can be minors where the child understands the basic significance of legal rights and obligations (this could be relatively young in real terms). Personal Data is information relating to an individual who can be identified from that information. The Courts have recently adopted a narrow interpretation of this definition and look to apply the Act to information which has the individual as its "focus" (rather than some other matter or person with which there may be a passing involvement) and which is "biographical in a significant sense" so as to affect the individual's privacy. Mere mention of a name on a document (perhaps as an email recipient for example) does not make that information (without more) Personal Data.

Schools are generally speaking, Data Controllers. As such they must notify the office of the Information Commissioner each year setting out in a template form the remit of the Data Processing which they undertake. Data Processing includes storing, gathering, sharing, using and even destroying Personal Data (such as that kept on parents, pupils, staff or others).

1. The Act includes 8 Data Protection Principles which must be adhered to at all times to ensure compliance. However, on occasion these can be interpreted with a common sense approach to ensure that a sensible balance is struck between the privacy rights of individuals and the need for Schools and alumni organisations to function as places of learning, support and as businesses.
2. Remember that the Act applies not only to Personal Data processed electronically (emails, computer records and so on) but also to manual paper-based records but only where these paper records are kept as part of a "Relevant Filing System". A Relevant Filing System of paper records must be highly sophisticated in its structure to the extent that only paper records which can be searched for specific pieces of information in the same way as a computer database search will be governed by the Act. This would exclude chronological collections of paper records or paper records which do not have a structure, index or search facility akin to a computer. This clearly cuts back the applicability of the Act so far as paper based records are concerned.
3. Individuals (including pupils) have rights of access to personal data held about them; rights to claim damages for breaches of the Act; rights in relation to direct marketing and decision taking and rights to correct inaccurate information. The Act includes a range of exemptions in relation to these rights some of which (exam results and references being two examples) will have a particular relevance for the Schools sector. Advice should always be sought in case of uncertainty.