Report on the data protection guidance we gave schools in 2012

ico.
Information Commissioner's Office

Contents

1. Background

During the first six months of 2012, the ICO helped schools in several local authority areas to comply with data protection rules by providing a specific report for each area recommending good practice.

To learn about their current data protection practice and awareness, the ICO asked all schools in the areas that took part to fill out a data protection self-assessment questionnaire. This gave us background information for the report and enabled schools to consider and review their answers. We've appended the questions we used in case they help other schools to self-review.

Over 400 schools in nine local authority areas returned completed questionnaires, which formed the basis of the individual reports.

This report draws together our findings. Its section headings are similar to those in the individual school reports and reflect the main areas on which we asked questions. Appendix 1 summarises the responses we received in these areas. We have included links to useful information from the ICO website where they are relevant to the work of schools.

2. Summary of recommendations

Here is a summary of our main recommendations under each section:

- Notification – make sure you notify us accurately of the purposes for your processing of personal data.
- Personal data – recognise the need to handle personal information in line with the data protection principles.
- Fair processing – let pupils and staff know what you do with the personal information you record about them. Make sure you restrict access to personal information to those who need it.
- Security – keep confidential information secure when storing it, using it and sharing it with others.
- Disposal – when disposing of records and equipment, make sure personal information cannot be retrieved from them.
- Policies – have clear, practical policies and procedures on information governance for staff and governors to follow, and monitor their operation.
- Subject access requests – recognise, log and monitor subject access requests.
- Data sharing – be sure you are allowed to share information with others and make sure it is kept secure when shared.
- Websites – control access to any restricted area. Make sure you are allowed to publish any personal information (including images) on your website.
- CCTV – inform people what it is used for and review retention periods.
- Photographs – if your school takes photos for publication, mention your intentions in your fair processing/privacy notice.
- Processing by others – recognise when others are processing personal information for you and make sure they do it securely.
- Training – train staff and governors in the basics of information governance; recognise where the law and good practice need to be considered; and know where to turn for further advice.
- Freedom of information – after consultation, notify staff what personal information you would provide about them when answering FOI requests.

3. Notification

Schools must notify the ICO that they are processing personal data. Our checks showed that not all schools were accurately notifying us of all the purposes for which they were processing personal data. You should make sure you do this and also renew your notification on time.

When a school has a notification with the ICO, it appears on the public register of data controllers. The data controller will be the school itself. (Technically it is the governing body, as the body corporate with responsibility for managing the school – but it is common, acceptable and more easily understood for notification to be done in the school's name.)

If your school gives an individual responsibility for data protection, they will be acting on your behalf. This is important because the data controller has responsibility under the Data Protection Act 1998 (DPA), not individual members of staff. Internal arrangements to delegate specific responsibilities are sensible, but this does not remove the data controller's responsibility.

As general advice, if you introduce any new purposes for processing personal information, such as installing CCTV to deter crime or disorder, you can easily add it to your notification. You can simply email our notification department (notification@ico.gsi.gov.uk), quoting your registration number – it usually begins with a 'Z' followed by seven digits (Znnnnnnn) – and ask for the new purpose to be added. There is no charge for this and we'll send you a copy of your revised notification.

Useful links
Register of Data Controllers

4. Personal data

The first step in processing personal data correctly is recognising it.

Personal data is information which relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.

The difference between processing personal data and sensitive personal data is that there are greater legal restrictions on the latter. You will hold sensitive personal data in pupil and staff records so you need to be aware of the extra care it requires.

You also need to differentiate between personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data) and personal information you can make freely available.

Example: the head teacher's identity is personal information but everyone would expect it to be publicly available. However, the head's home phone number would usually be regarded as private information.

The DPA requires you to strike the correct balance in processing personal information so that you respect individuals' privacy where it needs protection. The eight data protection principles are the key to finding that balance and ensuring compliance with the DPA. All schools should be aware of these principles. Most schools now use an electronic information management system and electronic communication, and many operate their own websites. Electronic processing of personal information is therefore the norm; however, schools are also likely to hold some information on paper.

In paraphrase, the principles require that personal data:

1. is processed fairly and lawfully;

2. is obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes;

3. is accurate and, where necessary, kept up to date;

4. is adequate, relevant and not excessive in relation to the purposes for which it is processed;

5. is not kept for longer than is necessary for those purposes;

6. is processed in accordance with the rights of data subjects under the DPA;

7. is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage; and

8. is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

Principles 1, 2, 6 and 7 tend to require the most careful consideration by data controllers when handling personal information.

Principles 3, 4 and 5 are principles of good records management, but remember that they are also legally required when the records hold personal information.

Principle 8 will rarely be of concern but it could apply if a pupil's family moves outside the European Economic Area.

5. Fair processing

Fairness includes being clear and transparent about how you will use the personal information you collect. To comply with the first and second principles, you should have in place a 'fair processing notice', sometimes referred to as a privacy notice.

You should give a fair processing or privacy notice to parents and pupils before or as soon as you obtain their personal information. The DPA does not prescribe a privacy notice's format – it could be in a school prospectus, an information pack, on a website or in a separate document. If you record personal details for specific purposes, say for counselling, you may need a privacy notice specifically for them. If you publish a general privacy notice on a website, you need to consider communication to families without easy web access. The important thing is to tell parents and pupils what personal information you are collecting and why. The links below show good and bad examples of privacy notices in the code of practice on privacy notices.

Make sure your notice mentions the purpose and use of any CCTV and the use you may make of photos of staff and pupils. Unless properly managed, friction can arise from putting identifiable images of pupils on a website or school publication – a form of processing personal data.

Fair processing – and avoiding unauthorised processing – also requires that you control access to personal information, giving access only to people (staff and governors) who need particular information to do their jobs, and only when they need it. This covers access to written and electronic staff and pupil records, and recorded CCTV images. So you need systems and procedures in place to control access to paper and electronic records containing personal information.

To ensure compliance, you should also monitor your controls. This is an important aspect of good information governance.

Useful links
Privacy notices code of practice
More information about personal data

6. Information security

Information security is probably the most important area for schools to concentrate on. The loss of or unauthorised access to personal information is likely to cause most harm to pupils, parents or staff and is most likely to result in us taking action. Individuals have a right to take action for compensation if loss of personal data causes them damage. The Information Commissioner now has the power to impose a monetary penalty for serious contraventions of the data protection principles. So not taking security seriously causes a reputational risk and could cost you money.

Physical security and procedures

You will already take security precautions over visitors to your school, which benefit staff and pupils alike. Another important aspect of good security relates to the physical security of, and restriction of access to, confidential personal information.

You should regularly review the physical security of buildings and storage systems, and access to them. This includes storage of paper records and the equipment used to store and process information electronically. If there are increased risks of vandalism or burglary, you should take these into account. Theft of a hard drive or damage to a router or server through which personal information is processed can seriously affect business continuity. If inadequate steps have been taken for protection, it also amounts to a breach of the data protection principles.

All portable electronic devices should be kept as securely as possible on and off school premises. If they contain personal information, they should be kept under lock and key when not in use. In addition to being financially prudent, this is also legally required if they hold personal information that could be considered confidential.

We advise that procedures should be in place, and be followed, when any personal information that could be considered in any way private or confidential is taken from the school premises in electronic or paper format. For paper records, this doesn't have to be a complex procedure. Something as simple as a booking-in-and-out process could reduce risks if used in all cases and monitored. More complex procedures may be needed for personal information held on portable electronic devices.

Electronic personal data

Strong passwords, i.e. at least eight characters long and containing special symbols, should be encouraged if any electronic equipment holds confidential personal information. We also recommend you set up a regular prompt to change your passwords and use different passwords for separate systems and devices.

We recommend you use encryption software to protect all portable devices and removable media, such as laptops and USB devices (or another form of memory storage not part of the computer itself), which hold confidential personal information. This is particularly important if they are taken from school premises. It is also important to prevent access to the information in case equipment is stolen. Memory sticks are easily lost, and laptops are attractive to thieves.

Encryption software uses a complex series of algorithms. The information on an encrypted drive is hidden from any unauthorised individuals who lack the pass code or key to the algorithm. Since encryption standards are always evolving, we recommend that data controllers ensure their solutions stay up to date and meet generally accepted standards.

There has been a spate of incidents where laptops containing personal information have been stolen from workplaces, vehicles and houses, or left in public places. After this, the Information Commissioner has decided that where such thefts or losses occur and encryption software has not been used to protect the data, enforcement action will usually follow.

Memory sticks are one of the main routes of data loss. They are convenient, portable and easy to lose or mislay. Either memory sticks should not be used to hold personal information or they should be password protected and fully encrypted. Buying encrypted memory sticks may seem expensive but can have two benefits. First, their high value may mean more thought is given as to whether they should be used. Second, the reputational damage and a monetary penalty for losing an unencrypted memory stick will be far more costly than buying an encrypted one.

Use of private computer equipment

Our survey showed it is common for some school staff and governors to use their own privately owned computer equipment for school business. This means the school itself will have little control over the security and disposal of such equipment. If any of the school's personal information is held on private equipment and something

goes wrong, the school will remain responsible unless it can prove it did everything reasonably possible to keep the information secure.

Paper-based personal data

Security of electronic data receives a lot of attention; less attention is sometimes paid to the physical security of paper-based personal data. Whenever possible, storage rooms, strong cabinets, and other storage systems with locks should be used to store paper records. Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access. As with memory sticks and laptops, particular care should be taken if documents have to be taken out of school.

Useful links
Security of personal information
Our approach to encryption

On our webpage giving advice for keeping information secure, there is a link to our advice on this topic for small and medium-sized organisations.

7. Disposal

The Data Protection Act 1998 does not give any specific guidance on how to dispose of personal data. Disposal is a form of processing that needs to be done fairly and the seventh principle states (this time in full):

'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

In deciding how to comply with the first and seventh principle when disposing of records in any form, the data controller must consider the nature of the information and the harm that may result from its unauthorised use. The method of destruction of personal data should take into account the nature of the information. In all cases you must ensure that data is disposed of in a way that creates little risk of an unauthorised third party using it to the data subject's detriment. If any confidential information is held on paper records, they should be shredded or pulped; electronic memories should be scrubbed clean or destroyed.

The ultimate responsibility for safely disposing of all electronic and paper records lies with the data controller. Remember this particularly if another organisation carries out this task for you.

Useful links
Information Security Principle 7

8. Policies

Spend some time ensuring that your school has clear and practical policies in all areas that affect good information governance. Written policies, backed up with written procedures if needed, help staff (and governors) to be aware of their responsibilities. As indicated above, three of the data protection principles relate to good records management. Good records management policies and procedures help you comply with the DPA. The seventh principle requires organisational methods to be in place to keep personal data secure. These methods are hard for you to demonstrate unless you have effective policies and procedures that you monitor and keep under review.

We recommend you give a specific member of staff responsibility for raising general data protection awareness and ensuring that policies are adhered to and updated as necessary. Consider spending some time during an inset day to raise awareness of policies and procedures.

Useful links
Data protection obligations

9. Subject access requests

Section 7 of the DPA gives individuals the right to request the personal information a school holds about them – the right of subject access. The definition of personal data for this purpose extends to any personal information held on record anywhere by the school (with one or two minor exceptions), and not just that held electronically, in structured files and in educational records. It includes information in correspondence and in notes made by governors, teachers and other staff. There are some exemptions to the right of access to information in certain records held by schools.

Subject access requests (SARs) need to be answered within 40 calendar days of receipt. You may charge a fee for answering a SAR. There is a standard fee of £10 and a sliding scale for information in educational records. A valid SAR should be in writing – this can include fax or email – and you should confirm the requester's identity.

Parents can make subject access requests on their children's behalf if the children are deemed too young to look after their own affairs or they have consented to their parents doing this on their behalf.

Handling subject access requests can be difficult and time consuming. Getting it right is important, particularly if other individuals' personal data is included in the information that should be provided to the requestor. We are not recommending that all schools have a member of staff fully trained in all the legal provisions and the exemptions that apply to subject access requests. Yet we do recommend that all schools can recognise a subject access request and know who to turn to for detailed advice to ensure compliance with the DPA.

Schools should keep a log of the requests that require formal consideration.

Subject access rights under the DPA are separate to the right of access to educational records under the Pupil Information Regulations for England, Northern Ireland, Scotland and Wales, which give a parent the right to information in their child's educational record. These regulations are outside the Information Commissioner's supervisory duties.

Useful links

Checklist for handling requests for personal information (subject access requests)

Individuals' rights of access to examination records
The use of biometric technologies in schools
Disclosure of exam results to the media

Access to pupil information in

- England
- Northern Ireland
- Scotland
- Wales

10. Sharing personal information

All schools share personal information with other organisations and usually with the same types of organisation. Sharing personal information involves providing it to another organisation or person so that they can make use of it. It does not extend to the use of personal information within the school, including use by the governing body.

The main organisations that schools share personal data with are:

- local authorities;
- other schools and educational bodies; and
- social services.

Personal information can be shared with pupils once they are old enough to be considered responsible for their own affairs, although information can also be shared with their parents or guardians. Pupils old enough to make decisions for themselves are entitled to have their personal information handled in accordance with their rights under the DPA rather than the rights of their parents acting on their behalf. So if this information is shared with parents, sharing must be in line with the data protection principles.

The three most important aspects to consider when sharing data are:

- making sure you are allowed to share it;
- ensuring that adequate security (taking into account the nature of the information) is in place to protect it; and
- providing an outline in a fair processing notice of who receives personal information from the school.

Method of transfer

You also need to consider how you provide personal information.

If you send an email containing personal data from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message. You may need to password-protect it and send the password separately. You should also check (and check again) that it is going to the correct email address and that you are sending only the information that needs to be sent. It is easy to attach the wrong document to an email.

Schools are increasingly using email to contact parents. As a way of communicating general information, it is cheap and convenient. But as mentioned above, it can present security difficulties if used to communicate confidential personal information. (Circular emails to parents should be sent bcc (blind carbon copy) so that email addresses are not disclosed to everyone.)

Similar considerations apply to the use of a fax machine. If you send confidential information by fax, you must make sure it goes to the right recipient and is not left unattended on their equipment, to be read by anyone who might pick it up.

Reports sent to us show that forgetting these simple checks often results in personal information getting into the wrong hands.

When sharing information with other organisations, secure methods are already available – for example the S2S system. Secure internal email systems may also be available within the local authority. Additionally, in some areas a few schools use the SIMS system, with secure access, for sharing information with parents. Schools should always consider using these or similar methods when sharing confidential personal data electronically.

Sharing paper copies of personal data or providing it on disk or memory stick also merits care to minimise the risk of loss. If you are sharing paper-based confidential personal information, you need to make sure it reaches the intended recipient. This is another reason to have a clearly defined policy for managing physical copies of personal data.

Useful links
Data sharing code of practice

11. Websites

A school website helps parents and pupils view information about your school, read your privacy notice and see what information you provide under your Freedom of Information Act publication scheme. If you post personal information, including images, on webpages available to all, you must comply with the data protection principles.

Four important considerations are:

1 Do not disclose personal information (including photos) on a website without the individual pupil, member of staff or governor being aware. We recommend you get consent before publishing photographs on a website.

2 On more sophisticated websites, where access to some sections is username and password controlled, you must take care to give only the necessary level of access and maintain strong password control. If you need to restrict access to part of the website, you should adequately protect this restricted information. Giving only the necessary level of access means making checks before doing so and ensuring access is stopped when no longer needed.

3 Be wary of metadata or deletions that could still be accessed in documents and images posted on a website.

4 There are now regulations in force about the use of cookies on websites.

Useful links
Personal Information Online Code of Practice

12. CCTV

An increasing number of schools have CCTV for security. We do not regulate the use of CCTV but can offer advice because it involves the processing of personal information. Capturing and/or recording images of identifiable individuals is processing personal information and it needs to be done in line with the data protection principles.

You need to be clear in your notification to us and in informing staff, pupils and visitors why you are collecting personal information in the form of CCTV images. If part of the purpose is to help maintain good order in the school, you need to mention this. You should site cameras only where they are needed for the stated purpose and where they do not unnecessarily intrude on anyone's privacy.

Give some thought to why you keep any recordings as well as having a set retention period based on the possible need to review the footage. Also consider who is allowed access to this footage and why. Remember that people can request CCTV images in subject access requests.

Useful link
CCTV code of practice 2008

13. Photographs

Schools may take photos for inclusion in a printed prospectus or other school publication without specific consent, as long as they have indicated their intentions. Take extra care if the photos to be published are of young pupils or if you intend to name individuals in a photo or put the pictures on a website.

Images captured by individuals for personal or recreational purposes, such as with a mobile phone, digital camera or camcorder, are exempt from the DPA. If a parent makes a video of their child in a school play for their own family use, this is not covered by data protection law. A school may still have a policy restricting the taking of photographs or other images (for instance, for child protection reasons or to prevent disturbance), but we stress that this is not a data protection issue.

If the school itself records the school play so it can sell the recordings to parents, it needs to make sure it is complying with the DPA.

Useful link
Read our guidance on taking photos in schools

14. Processing by others

For DPA purposes, a data processor is a person or organisation, not being a school employee, who processes personal information on the school's behalf. The school remains responsible for any processing that a data processor might do for it. The best way of ensuring compliance is to have a written agreement or formal contract with the data processor, covering the security of the personal information being processed.

As new technologies emerge, you need to be clear about what you are signing up to and risking when asking another organisation to process data for you.

Useful links
Outsourcing Guide

15. Training

Those making decisions about running schools need to know about information rights. Many data protection failures are caused by ignorance and anything that promotes awareness is to be recommended. Mistakes can often be prevented by being aware that a potential problem exists and knowing who can give more detailed advice.

Information governance is not optional. As electronic systems become more complex, capable and extensive, it is increasingly important to know how to safeguard the personal information they process. There should really be someone at, or accessible to, every school who has a working knowledge of information rights and records management linked to an understanding of the systems in use. All staff (and volunteers and governors) should receive some guidance on confidentiality of personal information, preferably linked to written policies.

To raise general staff awareness, consider arranging sessions on inset days. Clear policies for staff (as mentioned in section 8 'Policies' above) fall into this category as well, and inset days are again a good opportunity to reinforce these policies.

The ICO has a website giving advice and guidance on most things a school would need to know about data protection. Our helpline can also answer specific queries on data protection and freedom of information. The website and helpline are free.

ICO Website
ICO helpline: 0303 123 1113 (Mon-Fri 9am-5pm)

16. Freedom of Information Act / Environmental Information Regulations

The right of access to information held by public authorities was outside the scope of this exercise. However, all maintained schools and academies (as public authorities under FOIA and EIR) should have an approved publication scheme and need to reply to requests for information in line with this legislation.

As regards personal data protection, this legislation can present difficulties in deciding what personal information can or should be made publicly available. A relevant policy raises awareness in schools of the rights of access to information and can also cover in principle the approach to the release of personal information, particularly of staff and governors.

Appendices

Appendix 1 – Summary of responses

As we have assured schools that we will respect the confidentiality of the information they provided, this appendix is not a detailed analysis of the questionnaires. It provides a basic outline of some of the reasons for asking the questions and the replies we received. Where percentages are used, they are rounded figures.

To give us an idea of the amount of personal information being handled, we asked about the size of the schools and the number of pupils. Included in the replies were several from small schools serving small communities. We were pleased that these schools had shown enough interest in information governance to complete the questionnaire. We asked about special educational needs as files for such pupils will almost certainly hold sensitive personal data. There were pupils with special educational needs at all the schools that replied to this question.

Most schools (95%) said they provided some information to pupils and parents about what was done with the personal information they supplied.

We asked how schools identified and processed personal information. Nearly all the schools were now using a computer-based management system handling pupils' personal information. Fewer than 10% of schools reported using biometric data. Not all schools had password-controlled access to confidential parts of the management system. More than three quarters monitored access to the system. Governors and parents were rarely given access to the schools management system.

The range of data-protection-related policies varied considerably, with a few schools indicating no policies and a few indicating a full range of them. About three-quarters of the schools having policies monitored their operation and in some cases they reported to the governors on this monitoring.

Fewer than a third of the schools said they had received subject access requests for personal information. 10% of these said they had some difficulty replying to them.

All schools said they had controls in place for the reception of visitors. Most, but not all, schools had a member of staff responsible for the their information systems.

Storage facilities and arrangements for handling paper files containing personal information varied considerably. While most schools said files were locked away securely when not in use, some said this did not always happen. Just under half the schools had procedures for removing files from store. Nearly all schools were sure they had safe disposal methods for paper records.

We asked about the secure use of computer systems. Nearly all schools (about 98%) reported that systems were protected by password access, but about a third said that it would not necessarily be a strong password or that there would not be prompts to change it regularly. A few schools said all their portable devices were encrypted, while a few said none of them were. About 80% of schools used secure e-mail systems, and anti-virus software seemed to be in general use. Schools seemed less sure about the secure storage of portable devices than they were about paper files.

Not all schools were satisfied that when electronic devices were no longer required the memories were wiped clean before disposal.

There seemed to be some uncertainty about how much staff and governors might be using their own computer equipment for school business, although more than half said this was at least a possibility.

Training undertaken by staff and governors varied considerably. Some schools, mainly the smaller ones, said no-one at the school had received training in any of the five areas mentioned in the questionnaire; some said all four groups mentioned in the questionnaire had received training in all of the areas; most reported somewhere in between.

The majority of schools knew where information was being shared, but some reported that they did not fully understand their responsibilities when sharing or asking others to process it.

Most schools (over 90%) had their own website. Fewer than half of them had a secure area with controlled access. Some schools (about 15% of those with secure areas) seemed to give access to this part of the website without carrying out identity checks. Nearly all schools were confident they were publishing only information that should be publicly available and had the permission they needed for publishing information about, or images of, staff and pupils on their website.

About half the schools used CCTV. Most of these had external cameras only, although a few also had extensive internal coverage. Their procedures for storing recordings and giving staff access to images varied greatly, with 15% of schools saying they had no set period for keeping recordings.

Appendix 2 – Questionnaire

Protecting personal information
Questionnaire for schools

General information	
1.1 Name of school	
1.2 Please provide a contact email address	
1.3 In which local authority is your school?	
	Tick answer here
1.4 How many staff are employed by the school?	
<30	
31 - 120	
> 120	
1.5 How many pupils attend the school?	
< 200	
201-600	
> 600	
1.6 How many pupils have special educational needs?	
<10	
11 - 50	
> 50	
1.7 How do you tell pupils and parents what you do with their personal information? (tick any that apply)	
School website	
Individual letter or written notice	
School information pack	
Other	
None of above	
1.8 Does your school use biometric data?	
Yes	
No	
2. School management systems	
2.1 Does your school use a computer based	

management system (eg SIMS)?	
Yes	
No	
(If No go to section 3)	
2.2 Does the system store any of the following types of personal information? (Tick all that apply)	
Pupil names	
Pupil addresses	
Staff Names	
Staff addresses	
Medical details	
Family details	
Special needs details	
Disciplinary records	
Educational attainment	
Other (please detail below)	
2.3 Who has access to this system? (Tick all that apply)	
Headteacher	
Teaching staff	
Support staff	
Parents	
Pupils	
School governors	
2.4 Is access to confidential areas of the system securely controlled via log in and strong password (eg a combination of letters, numbers and other characters)?	
Yes	
No	
2.5 Is this access monitored?	
Yes	
No	
3. Policies	
3.1 Does the school have in place any of the following policies? (tick all that apply)	
Data protection policy	
Privacy policy	

Records management policy	
Records retention/disposal policy	
Information security policy	
Freedom of Information policy	
Policy for dealing with requests for personal information	
Policy for dealing with requests for general information	
3.2 Is adherence to these policies monitored?	
Yes	
No	
3.3 Who monitors these policies? (tick all that apply)	
Senior school staff	
School governors	
3.4 How many requests for personal information have been received by the school in the past 12 months? (This could be from pupils, parents or teachers)	
None	
1-10	
11-20	
>20	
3.5 Has the school replied to all the requests for personal information?	
Yes	
No	
4. Information security	
4.1 How is the school building kept secure on school days? (tick all that apply)	
One specific entrance for visitors	
Intercom system for visitors	
Sign in/out system at reception	
Security passes for visitors	
Keypad system on main internal doors	
Visitors accompanied at all times	
CCTV (outside school)	
CCTV (inside school)	
4.2 Do you have a member of staff who has specific responsibility for information systems?	
Yes with relevant training	
Yes but without relevant training	

No	
4.3 Where are paper files containing pupil (and parent) information stored? (tick all that apply)	
School office	
Headteacher's office	
Staffroom	
Classroom	
Corridors	
Storage room	
Other (please specify below)	
4.4 Are these paper files locked away when in not in use?	
Always	
Usually	
Sometimes	
Rarely	
Never	
4.5 Who has access to these paper files?	
Headteacher	
Teachers	
Support staff	
SENCO	
School governors	
4.6 Does the school have specific procedures for taking files out of storage?	
Yes	
No	
4.7 Does the school shred or pulp confidential paper records when no longer needed?	
Yes	
No	
4.8 Which of the following electronic devices are used by the school? (tick all that apply)	
Desktop computer	
Laptop	
Memory sticks	
Digital camera	
Smart phones	

4.9 Which of the following devices, where used, are encrypted?	
All desktop PCs	
Some desktop PCs	
No desktop PCs	
All laptops	
Some laptops	
No laptops	
All memory sticks	
Some memory sticks	
No memory sticks	
4.10 Are all school computers password protected ?	
Yes	
No	
(If no go to question 4.13	
4.11 Are computer users required to select a 'strong' password (ie a mixture of special characters, letters and numbers)?	
Yes	
No	
4.12 Are users prompted to change their password at regular intervals?	
Yes	
No	
4.13 Where are portable electronic devices kept when the school is closed? (tick all that apply)	
On desks	
In a drawer	
In a cupboard (unlocked)	
In a cupboard (locked)	
In a secure storeroom	
At the home of school staff	
4.14 Do you use only secure email systems to send and receive confidential information?	
Yes	
No	
Not sure	

4.15 Do all computers have anti-virus software installed?	
Yes	
No	
Not sure	
4.16 When unwanted electronic devices are passed on are the memories scrubbed clean or re-formatted?	
Yes	
No	
Not sure	
4.17 Does any member of staff or school governor use their own computer equipment for school business purposes?	
Yes	
No	
Not sure	
5. Staff training	
5.1 Who has received specific training in the following? (tick all that apply)	
Information rights	
Headteacher	
Teachers	
Support staff	
Governors	
None	
Information security	
Headteacher	
Teachers	
Support staff	
Governors	
None	
Records Management	
Headteacher	
Teachers	
Support staff	
Governors	
None	
Personal data protection	
Headteacher	
Teachers	
Support staff	
Governors	

None	
Freedom of information	
Headteacher	
Teachers	
Support staff	
Governors	
None	
6. Information sharing	
6.1 What other organisations do you share pupil information with? (tick all that apply)	
Social Services	
Other Local Authority departments	
Health services	
Ofsted/Estyn	
Schools/academic bodies	
Individual school governors	
Other (please specify below)	
6.2 Are you satisfied that all they use this information only for the reason it is provided?	
Yes	
No	
Not sure	
6.3 Are you satisfied that they keep this information secure?	
Yes	
No	
Not sure	
7. Website	
7.1 Does the school have it's own website?	
Yes	
No	
(If no go to section 8)	
7.2 Is access to any section of the website restricted?	
Yes	
No	

7.3 How is access to the restricted part of the website controlled?	
Login password provided by school after identity check	
Log in password provided on request	
7.4 Does the website have a link to a privacy policy	
Yes	
No	
7.5 Are you publishing any information (including images) staff, pupils or parents might object to?	
Yes	
No	
Not sure	
7.6 If your website has information or images of pupils or teachers do you have their permission to do this?	
Yes	
No	
Not sure	
8. CCTV	
8.1 Does the school operate a CCTV system?	
Yes	
No	
(If No you have now completed this questionnaire)	
8.2 Where is CCTV used? (tick all that apply)	
School grounds	
School corridors	
Classrooms	
Offices	
Storerooms	
Other (please specify below)	
8.3 How long do you store CCTV footage for?	
Don't store it	
< one month	
One month to three months	
> three months	
No set amount of time	

8.4 If stored, who has access to this footage? (tick all that apply)	
Specifically nominated members of staff	
Headteacher	
Caretaker/building manager	
Security staff	
Administrative staff	
All staff	
School governors	