Bournville Primary School

Data Protection and Information Sharing Policy

Date Ratified: 24th November 2015

Signed By:
On behalf of School Governors

Signed by :
Headteacher

Review Date: December 2016

Bournville Primary School
Data Protection and Information Sharing Policy

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, common law duty of confidentiality, current Information Sharing Guidance and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data need to be aware of their duties and responsibilities by adhering to these guidelines.

Information Governance refers to and encompasses the policies, procedures, processes and controls implemented to manage information. These support the school's immediate and future regulatory, legal, risk and operational requirements. Therefore the Data Protection and Information Sharing Policy is part of the Information Governance suite and should be read in conjunction with our E-Safety Policies, Safeguarding Children Policy, Whistle Blowing Policy and legislation and guidance referred to above.

Introduction

Bournville Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable us to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Bournville Primary School, as a Data Controller, is registered with the Information Commissioner's Office (ICO) detailing the information held and its use. We issue a Fair Processing Notice to all pupils/parents, which summarises the information held on pupils, why it is held and the other parties to whom it may be passed on to.

Bournville Primary School will do everything within its power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data to ensure it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

All personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the 'Conditions for Processing' (see appendix 6)

Any loss or misuse of personal data can have serious effects for both individuals with personal liability and / or institutions concerned, as it can bring the school into disrepute and may well result in disciplinary action and / or fines and/or criminal prosecution.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles"**.** (Please see Appendix 1 for Subject Access Request Procedures.)

Responsibilities

The school's Business & Strategic Resource Lead will undertake the role of Senior Information Risk Officer (SIRO). This person will keep up to date with current legislation and guidance and will:
-determine and take responsibility for the school's information risk policy and risk assessment
-appoint the Information Asset Owners (IAO's)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. Pupil/Student Information / Staff Information / assessment data etc). The IAOs will manage and address risks to the information and will understand:
-what information is held, for how long and for what purpose
-how information has been amended or added to over time
-who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data when engaged in their role as a Governor.

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers - the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform Parents/Carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, DfE etc) to whom it may be passed. This privacy notice will be passed to Parents/Carers through the school website. Parents/Carers of young people who are new to the school will be provided with the privacy notice through school website or letter.

Training and Awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:
-induction training for new staff
-staff meetings / briefings / inset
-day to day support and guidance from Information Asset Owners

Personal Information

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

The school has access to a wide range of personal information and data. The data may be held in different formats such as digital or paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.

This will include:

- Personal information of a private or sensitive nature about members of the school community – including pupils, parents and carers, also members of staff and other professionals eg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records

- Curricular / academic data eg class lists, pupil / student progress records, reports, references

- Professional records eg employment history, taxation and national insurance records, appraisal records, health forms and references

- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members and shared in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

- Information that is not already lawfully in the public domain

Sensitive Personal Data

Sensitive personal data consists of information relating to the racial or ethnic origin of a data subject, their political opinions, religious beliefs, trade union membership, sexual life, physical or mental health or condition, or criminal offences or record.

Where the school, as Data Controller intends to process sensitive personal data, there are further conditions. If none of the following conditions can be met, processing cannot legally continue;

- where the data subject has given his explicit consent;
- where the processing is required for the purposes of complying with employment law;
- where it is necessary to establish, exercise or defend legal rights.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures
- Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator). Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745 3

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system or to all records.

All ICT users will be given secure accounts and must create strong passwords which must be implemented in accordance with the school's E-Safety Policy, regarding Password Security. These passwords must be changed regularly. User passwords must never be shared.

Personal data may only be accessed on school devices which are securely password protected.

Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation. The school promotes a clear desk approach to ensure information of a personal or sensitive nature is not available for unauthorised access.

Personal data can only be stored on school servers or equipment (this includes computers and portable storage media where allowed). No information of a sensitive nature can be kept on a member of staff's personal drive eg ..... drive, unless agreed by the Head teacher, Data protection officer and that the technician is informed.

Private equipment (ie owned by the users) must not be used for the access or for the storage of personal data. It is the responsibility of the member of staff to ensure any private equipment used to open school emails and attachments of a confidential nature by remote access, does not retain any information on the hard drive.

When personal data is stored on any portable computer, USB stick or any removable media:
-the data must be encrypted and password protected
-the device must be password protected
-the device must offer approved virus and malware checking software
-the data must be securely deleted from the device, in line with the school policy once it has been transferred or it's use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote/cloud based data services providers to protect the data.

As a Data Controller the school is responsible for the security of any data passed to a 'Third Party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The school recognises under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them: a description of that data: the purpose for which the data is processed: the sources of that data: to whom the data may be disclosed and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification , blocking, erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other multi-agency organisations. In these circumstances:

- Users may not remove RESTRICTED data from the school or authorised premises without permission from the Senior Management Team and unless the media is encrypted and password protected and is transported securely for storage in a secure location. CONFIDENTIAL information may only be removed with agreement from the Head teacher.

- Users must take particular care that computers or removable devices which contain personal data to ensure that they are not be accessed by other users (eg family members) in or out of school.

- When sensitive or personal data is required by an authorised use from outside the school's premises (for example, by a member of staff to work from their home), users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is school-issued, encrypted and is transported securely for storage in a secure location and returned to the secure area of the school onsite network.

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

- If sensitive or personal data is removed from school premises, such as files for safeguarding meetings, school trips etc the Removal of Data log must be completed when removing information and on return.

- (Other secure options will be explored including use of secure remote access to the management information systems).

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of data deemed protected or higher, in either paper or electronic form, will be conducted in a way that makes reconstruction highly unlikely. A normally deleted file can be recovered, even if the file is later overwritten by a new one. Electronic files will be securely overwritten (generally seven times as in encrypted software), in accordance with government guidance and other media will be shredded, incinerated or otherwise disintegrated.

A Destruction of Data Log will be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

The activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by the Head teacher and Data Protection Officer.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches, for example; loss of protected data or breaches of an acceptable usage policy, or filtering changes.

The Data Protection Officer will maintain an inventory of, and will audit all school ICT equipment such as desktop and laptop computers and all portable devices eg cameras, mobile phones.

Members of staff who are leaving must return all personally-issued ICT equipment to the the Data Protection Officer. The Data Protection Officer and technician must be notified of staff leavers to ensure all school equipment is returned. Staff who are leaving will be required to sign a declaration , countersigned by the Head teacher and Data Protection Officer, confirming they have returned all school equipment and property, also that they will not attempt to access school information after their leaving date and that their personal ICT equipment will be appropriately configured to prevent unauthorised access to personal or sensitive information (see Appendix 5).

Information Risk Incidents

All data protection incidents must be reported immediately to the Head teacher and Data Protection Officer. The Head teacher will report breaches to North Somerset Council and work in conjunction with the council to devise a plan of action for rapid resolution. A plan of action to prevent recurrence and further awareness raising will also be developed.

ICT Service Continuity Management

The school has an ICT Service Continuity Plan that provides the framework for the school to develop a plan that considers the preparation for, response to and recovery from a disaster affecting all (or part) of the range of critical data held in the school's management information systems.

Protected Marking

Following national incidents involving loss of data, the Government Protective Marking Scheme, will be used to indicate the sensitivity of data.

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (physical or digital) that contain PROTECT or RESTRICT data will be labelled clearly in a footer, together with release or destruction dates if allocated and known. Emails containing data that falls into the PROTECT OR RESTRICT categories will be marked as such and will not be sent externally, except where the intended recipient is authorised to receive the email, the secure email system (using encryption) is used and the SLT has authorised the email.

All paper based PROTECT or RESTRICT (or higher) material must be held in lockable storage.

Bournville Primary School is aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. (Please see Appendix 4)

Disclosure of educational records

Schools, as independent public bodies, are directly responsible under the Data Protection Act 1998 (DPA) for the collation, retention, storage and security of all information they produce and hold. This will include educational records, head teacher's reports and any other personal information of individuals - pupils, staff and parents.

The Pupil Information Regulations 2005, require that a school's governing body ensures that a pupil's educational record is made available for their parent to see, free of charge, within 15 school days of receipt of the parent's written request. If a parent makes a written request for a copy of the record this too must be provided and within 15 school days. Governing bodies can charge a fee for the copy but if they do, it must not be more than the cost of supply.

Information Sharing

Information Sharing is a key element of safeguarding children and young people. Bournville Primary School will explain to students and their families what and how information will or could be shared, with whom and why, and also seek their agreement when required.

Personal information of a private or sensitive nature relating to children within a class, is only for the use of the teacher, supply staff, and other staff or professionals, who need to know and who work with the child. It is the responsibility of the class teacher to ensure appropriate information is shared effectively, appropriately, legally and professionally.

The personal information must only be shared with other professionals, relevant support staff or other teachers in this school for genuine purposes, for example, to seek advice on a particular case or ensure cover for work while on leave.

It is the class teacher's responsibility to share confidential information appropriately, with their team both permanent and temporary. This is to ensure children's care, safety and well-being, so must be the overriding consideration in making any decisions.

Any decision to share, or not share, information must be recorded, detailing the reason for the decision, what information has been shared, with whom and for what purpose. This record must be held with the child's record.

If confidential information is shared, as outlined above, this must be in a professional manner to ensure compliance with current Information Sharing Guidance and the Information Sharing Policy and protocols.

Whilst parents have a right to expect that personal information they share with Bournville Primary School will be regarded as confidential there are, however, certain circumstances when information can be shared without parents' consent, such as when;

- there is evidence that the child is suffering, or is at risk of suffering, significant harm.
- there is reasonable cause to believe that a child may be suffering, or at risk of suffering significant harm.
- failing to do so would put a pupil at increased risk of significant harm,
- it would undermine the prevention, detection or prosecution of a serious crime.

When sharing information without consent, Bournville Primary School will always consider the safety and welfare of a pupil in making the decision. When there is a concern that a pupil may be suffering, or is at risk of suffering, significant harm, the student's safety and welfare will always be the overriding consideration. It is the responsibility of the designated Child Protection Officer to decide and provide authorisation to staff seeking to make a disclosure. (Please see Appendix 2 and 3.)

If information is shared, this will be recorded in the student safeguarding file in the following way: What information was provided and to whom, the reason for sharing information and the name of the Designated Child Protection Officer disclosing the information together with the member of the Senior Leadership Team who authorised disclosure of information.

All information shared will be in accordance with current Information Sharing Legislation and Guidance, also Data Protection Act principles of being up to date, necessary for the purpose for which it is being shared and shared only with people who need to see it. It will only be shared in a secure manner in line with the school's E-Safety Policy.

Appendix 1

Rights of access to information

There are three distinct rights of access to information held by schools;

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them. This right is commonly referred to as subject access requests (SARs), is created by Section 7 of the Data Protection Act. It can be used by individuals who want to see a copy of the information the school holds about them. They can request to be;

- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and
- given details of the source of the data (where this is available).

2. The right of those entitled to have access to curricular and educational records as defined within the Education Records Regulations 2005 and 2008. The Pupil Information Regulations require that a school's governing body ensures that a pupil's educational record is made available for their parent to see, free of charge, within 15 school days of receipt of the parent's written request. If a parent makes a written request for a copy of the record this too must be provided and within 15 school days.

The procedures to follow are the same as for Subject Access Requests, however the time scales and fees differ. Bournville Primary School Governing body may charge a fee for the copy but if they do, it must not be more than the cost of supply – see section 4.

3. A Freedom of Information request can be initiated by any person. The information disclosed through an FOI request will usually become public information, available to anyone. The response cannot, therefore include personal or sensitive information, as these are exempt from FOI requests. This may be subject to a fee, to be determined, on a case by case basis by the governing body.

Actioning a Subject Access Request , Pupil Information or Freedom of Information Request

1. Requests for information must be made in writing; which includes email, and be addressed to the Head teacher. See appendix 7 - Subject Access Request Form. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any personal or sensitive information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of at least two of the following, to establish identity and current address :

- passport
- driving licence
- utility bills with the current address

- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head teacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records to be disclosed. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Of the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Head teacher.
- Should the information requested be personal information that does not include any information contained within educational records the school can charge up to £10 to provide it.

5. The response time for Subject Access Requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However the 40 days will not commence until after receipt of fees, identification and clarification of information sought

6. The response time for Pupil Information requests, once officially received, is 15 days (not working or school days but calendar days, irrespective of school holiday periods). However the 15 days will not commence until after receipt of identification and clarification of information sought, if required.

7. The response time for Freedom of Information requests, once officially received, is 15 days (not working or school days but calendar days, irrespective of school holiday periods). However the 15 days will not commence until after receipt of fees and clarification of information sought

8. The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure by the Head teacher.

9. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale for SARs.

10. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information

that would reveal that the child is at risk of abuse, or information relating to court proceedings.

11. If there are concerns over the disclosure of information then additional advice should be sought.

12. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

13. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

14. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Appendix 2

Seven Golden Rules for Information Sharing

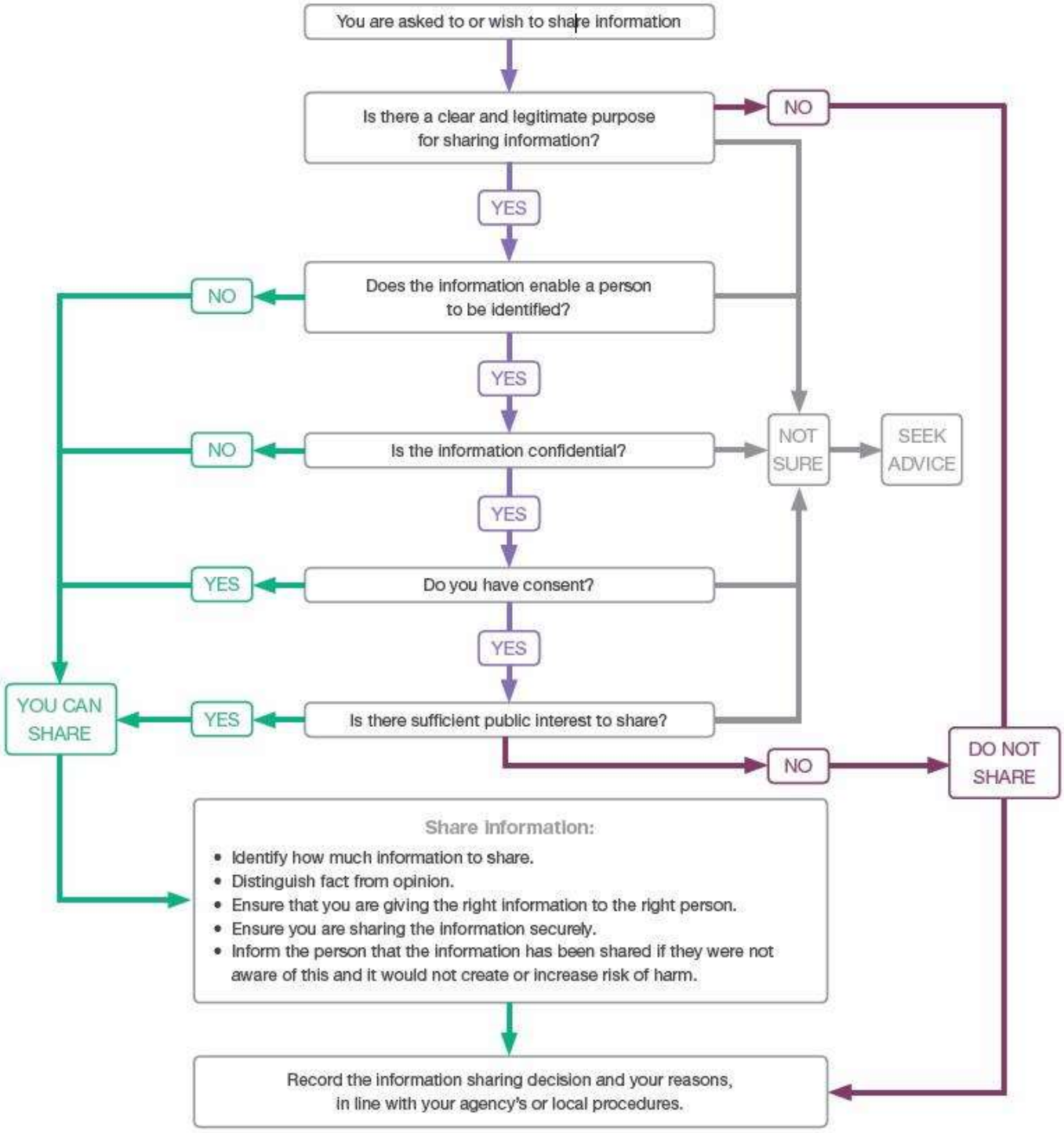
Seven golden rules for information sharing

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.
2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.
4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Local contacts

Extract from HM Government *Information Sharing: Guidance for practitioners and managers.*
Copies can be obtained from **www.ecm.gov.uk/informationsharing**

Flowchart of key questions for information sharing



Appendix 3

Data Sharing Checklists: https://ico.org.uk/media/for-organisations/documents/1067/data_sharing_checklists.pdf

Data sharing checklists

These two checklists provide a handy step by step guide through the process of deciding whether to share personal data. One is for systematic data sharing, the other is for one off requests.

Then checklists are designed to be used alongside the full code and highlight the relevant considerations to ensure that the sharing complies with the law and meets individuals' expectations

Data sharing checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified?

Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

It is good practice to have a data sharing agreement in place.

As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Data sharing checklist – one off requests

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified?

Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

Key points to consider:

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared securely.
  - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

Appendix 4

Handling Information based on the Protective Marking

	OFFICIAL	OFFICIAL SENSITIVE
INFORMATION MARKING		
Legal and statutory obligations, in particular under the Data Protection Act, will be followed whatever the protective marking used.		
General points	• Be stored and managed securely • Handled in line with clear desk policy (Red folders and laptops locked when not in use) • Not be accessed, read or discussed where you can be overlooked or overheard	• Not be left unattended and should be filed away (in Red folders) when not in use • Only communicated or passed to others on a need to know basis
Emailing material	• By default this information can be sent in the clear over the internet • No restrictions on emailing information, however it should be limited on a 'need to know' basis • You may choose to include additional handling guidance/instructions if appropriate • When receiving email you must follow any handling guidance stipulated by the sender • Where necessary adopt the transmission technique as used by the sender (eg encryption of message if sending outside your email domain) • Where information you have added has increased the sensitivity you may choose to password protect or encrypt to provide additional protection	• Permitted to known contacts on a 'need to know' basis • You must follow the document originator's lead on encryption when replying to or forwarding emails • Information should normally be sent by encrypted email • Use password protection when encryption is not appropriate

<table>
<tr><td>Moving information by hand or post</td><td>By Hand:
Protect at least by one cover/envelope
Authorisation should be obtained from the Information owner if moving a significant volume of records
By Post:
Use single, unused envelope</td><td>Carry in a nondescript bag in order to not draw attention to the contents
Never leave papers unattended
Include return address on back of the envelope
Never mark the classification on the envelope
Consider double envelope for highly sensitive data
Consider using registered Royal Mail service or reputable commercial courier’s ‘track and trace’ service.</td></tr>
<tr><td rowspan="2">Faxing</td><td colspan="2">Faxes should not assumed to be secure. Consider using encrypted email if possible to communicate sensitive information.</td></tr>
<tr><td>Confirm the recipient’s fax number
Recipients should be waiting to receive faxes containing personal data marked OFFICIAL</td><td>Sensitive material to be faxed should be kept to an absolute minimum</td></tr>
<tr><td>Printing</td><td colspan="2">Permitted – but print only what you need and consider PIN protected printing
All printed materials must be disposed of appropriately when no longer required or being used</td></tr>
<tr><td>Photocopying</td><td colspan="2">Permitted – but make only as many copies as you need, and control their circulation
Consider PIN protected printing/copying where appropriate</td></tr>
<tr><td colspan="3">STORAGE</td></tr>
<tr><td>Physical Storage (of documents, digital media, when not in use)</td><td colspan="2">All OFFCIAL and OFFICAL SENSITIVE data to be filed in RED FOLDERS
Laptops and computers must be locked to user/logged out when unattended</td></tr>
</table>

Electronic Storage	• Any electronic document received marked OFFICIAL should be saved with OFFICAL in the title and also in electronic document and records • Appropriate controls should be used to limit access	• Any electronic document received marked OFFICIAL SENSITIVE should be saved with OFFICIAL SENSITIVE in the title and also in electronic document and records management • Appropriate controls must be used to limit visibility of the document and access
Electronic storage on digital media (USB memory sticks, CDs, DVDS	• Personal memory equipment must not be used for OFFICIAL or OFFICIAL SENSITIVE data • School portable memory equipment must be encrypted and permission from Data Controller approved • Delete protectively marked information held on digital media whilst on school equipment only	
Disposing of documents	Dispose of documents appropriately. • Information already in the public domain can be disposed of by recycling or in general waste • Information marked OFFICIAL or OFFICIAL SENSITIVE must be disposed of with care, either using the office 'Green confidential waste bag' or by shredding (cross-cut)	
REMOTE WORKING		
General points	• Laptops and removable media used to store OFFICIAL or OFFICIAL SENSITIVE information must be encrypted • Information marked OFFICAL or OFFICIAL SENSITIVE must not be emailed to or from home/personal email accounts • Limit the amount of information you take out of school Refer to Acceptable User Policy on Bring Your Own Device and acceptable working practises.	
Telephone, videoconferencing etc	You should not assume telephony systems, video conferencing or tools such as Skype are secure.	
	• No restrictions but be careful how your discussion might be perceived by others in earshot and of straying into areas that could be seemed as OFFICIAL SENSITIVE.	• Details of OFFICIAL SENSITIVE material should be kept to an absolute minimum and should only be discussed where there is no risk of being overheard

Risk Assessments

Information risk assessments will be carried out by the E-Safety Committee as Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences)
- Prioritising the risks

Impact Levels and protective marking

The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	**Impact Level (IL)**					
		Very unlikely	Unlikely	Possible	Likely	Frequently
NOT PROTECTIVELY MARKED	0					
PROTECT	1 and 2	Low	Low	Medium	Medium	Medium
RESTRICTED	3	Low	Medium	Medium	Medium	High
CONFIDENTIAL	4	Medium	Medium	Medium	High	High
HIGHLY CONFIDENTIAL	5					
TOP SECRET	6					

Use of technologies and Protective Marking

The following (from Becta and SWGfL) provides a useful guide:

	The information	**The technology**	**Protect Markings (Impact Level)**
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publicly accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual learner's academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs. CHPs, Annual Reviews, Statement of Educational need, Child Data, Child Risk Assessments, Children's work, Home School Diaries, IEPs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Learners whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this learners record available in this way.
Safeguarding	Child Protection and Safeguarding information, Staff Support Records.		CONFIDENTIAL

Risk Assessment is an ongoing process and should result in the completion of an Information Risk Actions Form (example below)

Appendix 5

Data Protection and Information Sharing Policy

Bournville Primary School Staff - Leaver Data Protection Declaration

Please sign below to agree that:

- I have returned all school equipment and property
- I will not attempt to access school information after my leaving date
- I am not in possession of any personal or sensitive data relating to school
- My personal ICT equipment will be appropriately configured to prevent unauthorised access to any school personal or sensitive information

Name:

Signature:

Date:

Name of Data Protection Officer:
Signature:

Name of Head Teacher:
Signature:

Appendix 6

Conditions for processing

The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

- The individual whom the personal data is about has consented to the processing.

- The processing is necessary:
    - in relation to a contract which the individual has entered into; or
    - because the individual has asked for something to be done so they can enter into a contract.

- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).

- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions

- The processing is in accordance with the "legitimate interests" condition.

Appendix 7

Subject Access Request Form

Section 1

This form is used by Bournville Primary School to help you to receive information we hold and process about you, the data subject (the term used for the person whose information is held by the school).

Please complete the form as fully as possible - if you do not it could make it difficult for us to process your request.

If you are applying on behalf of another person, with their consent, **please include proof of your right to do so.** If you need help completing this form please contact ***The Headteacher***

Data subject's name _____

Address _____

_____Post code_____

Previous address if you have moved since your details were given to the school:

_____

_____Post code_____

Section 2 (Please circle)

Are you the data subject named above?	**Yes/ No** (If yes please proceed to section 4)
Are you the parent/guardian of the child pursuing your separate right to access your Child's official educational records?	**Yes/ No** (If yes please proceed to section 4)
Are you the parent/guardian of the child and acting on behalf of a child does not understand the nature of their own access rights?	**Yes/ No** (If yes please proceed to section 3)
Are you acting on behalf of the person named above?	**Yes/ No** (If yes please proceed to section 3)

Section 3 - If you are acting on behalf of the data subject

Do you have written permission?	**Yes /No** If yes please attach a copy and proceed to section 3a.

Section 3a - Please complete the following declaration

I …… (Applicant) declare that **I am an agent** acting on behalf of the data subject with their full knowledge and written consent (enclosed), or on behalf of a child who does not understand the nature of the request and I am acting in their interest. I will only disclose the information to the data subject except with further authorisation from them.

Signed ……Agent / Parent……...

Section 3b - Details about the agent

Data subjects name_____

Address_____

_____ Postcode _____Tel_____

Section 4 – Details of the information required

Please state in your own words what information you require, include details of any reference numbers given to you like payroll or client numbers, or reasons why you believe the school has your personal information in its files.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Section 5 - Declaration to be signed by all applicants

I declare that the information given in this form is correct and that I am the data subject, parent or agent.

Signed…… Date……

The school has 15 school days to respond to a request for educational records and 40 calendar days to respond to other requests. The information you provide on this form will be used only for the purposes of processing your request.