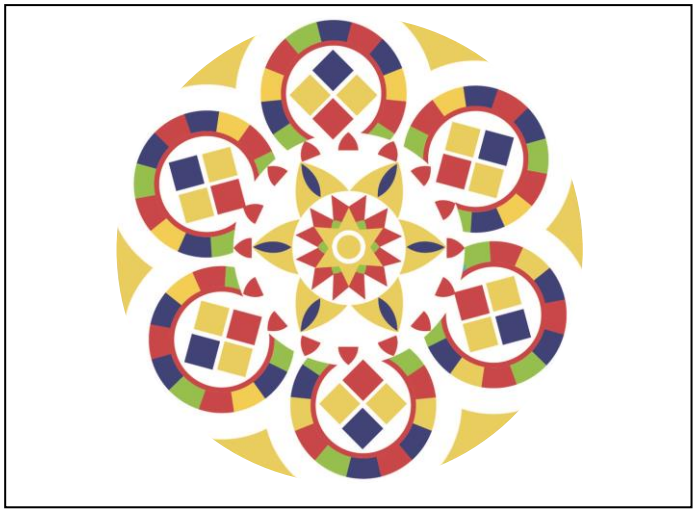
SPARKENHOE COMMUNITY PRIMARY SCHOOL



General Data Protection Policy

Policy Date:	July 2018		**Version:** 1.2		
Policy Review Date:	July 2019		Headteacher Name R Jones	Signature	Date 2.7.18
Ratified by Governing Body: 2nd July 2018 at Full Governing Body meeting					
L Jowett			Signature	Date 2.7.18	

Introduction

In order to operate efficiently Sparkenhoe Community Primary School has to collect and use information about people with whom it works and the pupils it provides an education to. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

The School is required to process relevant personal data regarding individuals as part of its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

Everyone has rights with regard to the way in which their personal data is handled. During the course of the School's activities it collects, stores and processes personal data about staff, pupils, their parents, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

The School is committed to ensuring personal data is properly managed and that it ensures compliance with current data protection legislation. The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

Those who are involved in the processing of personal data are obliged to comply with this Policy when doing so. Any breach of this Policy may result in disciplinary action.

The policy meets the requirements and expectations of the General Data Protection Register introduced in law as of the 25th May 2018.

1. Scope

This policy applies to all employees, governors, contractors, agents and representatives, volunteers and temporary staff working for or on behalf of the School.

This policy applies to all personal data created or held by the School in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, workbooks, email, filing cabinet, shelving and personal filing drawers).

Personal data is information about living, identifiable individuals, or an identifier or identifiers that can be used to identify a living individual. It covers both facts and opinions about the individual. Such data can be part of a computer record or manual record.

Current data protection legislation does not apply to access to information about deceased individuals. However, the duty of confidentiality may continue after death.

See appendix 2 for a list of terms and definitions

2. Responsibilities

Overall responsibility for ensuring that the School meets the statutory requirements of any data protection legislation lies with the Governors and the Chair of Governors has overall responsibility for information management issues. They have delegated the day-to-day responsibility of implementation to the Headteacher.

The Headteacher is responsible for ensuring compliance with data protection legislation and this policy within the day-to-day activities of the School. The Headteacher is responsible for ensuring that appropriate training is provided for all staff.

All contractors who hold or collect personal data on behalf of the School by way of written contract are responsible for their own compliance with data protection legislation and must ensure that personal information is kept and processed in line with data protection legislation and only upon instruction from the school, via a contract.

3. The Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice as enshrined within the requirements of the GDPR.
These provide that personal data must be:

- ✓ Fairly and lawfully processed
- ✓ Processed for a lawful purpose
- ✓ Adequate, relevant and not excessive
- ✓ Accurate and up-to-date
- ✓ Not kept for longer than necessary
- ✓ Processed in accordance with the data subject's rights
- ✓ Secure
- ✓ Not transferred to other countries without adequate protection

4. Notification

The Digital Economy Act 2017 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the School must be registered.

The School will review the Data Protection Register (https://ico.org.uk/esdwebpages/search) annually, prior to renewing its notification to the Information Commissioner.

5. Types of Personal Data Processed by the School

Personal data covers both facts and opinions about an individual. The School may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including, by way of example:

As detailed on the **Sparkenhoe Parental Data Consent Form (appendix 1)**

- ✓ Names, addresses, telephone numbers, email addresses and other contact details
- ✓ Past, present and prospective pupils' academic, disciplinary, admissions and attendance
- ✓ records (including information about any special needs), and examination scripts and marks
- ✓ Where appropriate, information about individuals' health, and contact details for their next of kin
- ✓ References given or received by the School about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils
- ✓ Images of pupils (and occasionally other individuals) engaging in School activities
- ✓ images captured by the School's CCTV system (in accordance with the School's policy on taking, storing and using images of children)

Generally, the School receives personal data from the individual directly (or, in the case of pupils, from parents). However in some cases personal data may be supplied by third parties (for example another School, or other professionals or authorities working with that individual), or collected from publicly available resources.

6. Sensitive Personal Data

The School may, from time to time, need to process sensitive personal data regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the School with the explicit consent of the appropriate individual, or as otherwise permitted by the Act. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the DPO for more information on obtaining consent to process sensitive personal data.

7. Keeping in Touch and Supporting the School

The School will use the contact details of parents, alumni and other members of the school community to keep them updated about the activities of the School, including by sending updates and newsletters, by email and by post.

8. Privacy Notices

Whenever information is collected about individuals they must be made aware of the following at that initial point of collection:

- The identity of the data controller, e.g. the School;
- Contact details of the Data Protection Officer;
- The purpose that the information is being collected for;
- Any other purposes that it may be used for;
- What the lawful basis is for processing the data;
- Who the information will or may be shared with;
- If the data is transferred outside of the EU, and if yes, how is it kept secure;
- How long the data will be kept for;
- How data subjects can exercise their rights.

The School will review its Privacy Notice annually and alert pupils and parents to any updates.

9. Conditions for Processing

Processing of personal information may only be carried out where one of the conditions of Article 6 of the GDPR has been satisfied.

Processing of special category (sensitive) personal data may only be carried out if a condition in Article 9 of the GDPR is met as well as one in Article 6.

10. Data Protection Officer

The School has appointed **Mrs P Cooper** as Data Protection Officer (DPO), who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the Act. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the DPO.

11. Data Protection Impact Assessments

The School shall undertake high risk Data Protection Impact Assessments in line with the requirements of the GDPR and as per the Information Commissioner's Office (ICO) guidance.

12. Data Breaches

All employees, governors, contractors, agents and representatives, volunteers and temporary staff shall report a security incident or data breach immediately to senior management and the School's Data Protection Officer.

The School shall report any personal data breach to the ICO in line with the requirements of the GDPR.

13. Contracts

The School shall ensure that a legally binding contract is in place with all of its data processors in line with the requirements of the GDPR.

14. Consent

Where the School processes data with consent (for example, to publish photographs of children, to send direct marketing emails about school uniform for sale) it will ensure that the consent is freely given, specific, informed and unambiguous**,** and the consent is recorded

15. Information Society Services

Where the School offers Information Society Services (online services with a commercial element) targeted at children, it will take reasonable steps to seek the consent of the child's parent or guardian if the child is under 13 years of age

16. Direct Marketing

Where the School sends any direct marketing (the promotion of aims and ideals as well as selling goods and services) via electronic communications e.g. email, SMS text, fax or recorded telephone messages, it will only do so if the recipient has given explicit consent to receive them e.g. has ticked a box to 'opt in'.

17. Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- Other members of staff on a need to know basis;
- Relevant Parents/Guardians;
- Other authorities if it is necessary in the public interest, e.g. prevention of crime, safeguarding;
- Other authorities, such as the Local Authority and schools to which a pupil may move, where there are legitimate requirements (DfEE leaflet 0015/2000 entitled "Pupil Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other schools. DfES/0268/2002 provides further information).

The School should not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Where there is doubt, or statutory requirements conflict, legal advice should be obtained. Where there are safeguarding concerns, the matter should be referred to the School's Designated Safeguarding Lead (DSL).

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled. Care must always be taken when there is any doubt about parental responsibility.

18. Rights of Access to Personal Data ('Subject Access Request')

Individuals have the right under the Act to access to personal data about them held by the School, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within statutory time limits (one month). They are entitled to see if the data held are accurate, and who it is shared with.

It should be noted that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts (though examiners' comments may be disclosed), nor any reference given by the School for the purposes of the education, training or employment of any individual.

When a request is received it must be dealt with promptly; a response must be provided as soon as possible and within one month and in some instances, for education records, 15 school days. All staff must recognise and log such a request with the Data Protection Officer.

The School cannot charge for responding to a subject access request unless the request is repeated manifestly unfounded or excessive. The School can charge up to £50 (on a sliding scale for photocopying charges) for access to a pupil's Educational Record.

When providing the information the School must also provide a description of why the information is processed, details of anyone it may be disclosed to and the source of the data.

Staff of the School must also recognise and log the following requests with the Data Protection Officer, and all must be answered within one month:

1. Right of Access.
Individuals have the right to obtain confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to that personal data.

2. Right to Rectification.
Individuals have the right to obtain rectification of inaccurate personal data and the right to provide additional personal data to complete any incomplete personal data.

3. Right to Erasure ("Right to be Forgotten").
In certain cases, individuals have the right to obtain the erasure of their personal data.

4. Right to Restriction of Processing.
Individuals have the right to obtain a restriction of processing, applicable for a certain period and/or for certain situations.

5. Right to Data Portability.
Individuals have the right to receive their personal data and they have the right to transmit such personal data to another controller.

6. Right to Object.
In certain cases, individuals have the right to object to processing of their personal data, including with regards to profiling. They have the right to object at further processing of their personal data in so far as they have been collected for direct marketing purposes.

7. Right to be Not Subject to Automated Individual Decision-Making.
Individuals have the right to not be subject to a decision based solely on automated processing.

8. Right to Filing Complaints.
Individuals have the right to file complaints about the processing of their personal data with the relevant data protection authorities.

9. Right to Compensation of Damages.
In case of a breach of the applicable legislation on processing of (their) personal data, individuals have the right to claim damages that such a breach may have caused with them.

Exemptions

Certain data is exempted from the provisions of the Act, including the following:

- ✓ The prevention or detection of crime
- ✓ The assessment of any tax or duty
- ✓ Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School
- ✓ Information which might cause serious harm to the physical or mental health of the pupil or another individual
- ✓ Cases where the disclosure would reveal a child is at risk of abuse
- ✓ Information contained in adoption and parental order records
- ✓ Information given to a court in proceedings under the Magistrates' Courts (Children and Young Persons) Rules 1992
- ✓ Copies of examination scripts; and
- ✓ Providing examination marks before they are officially announced

Further exemptions may include information which identifies other individuals, information which the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The School will also treat as confidential any reference given by the School for the purpose of the education, training or employment, or prospective education, training or employment of any pupil. The School acknowledges that an individual may have the right to access a reference relating to them received by the School. However such a reference will only be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent or if disclosure is reasonable in all the circumstances.

19. Whose Rights?

The rights under the Act are those of the individual to whom the data relate. However, the School will, in most cases rely on parental consent to process data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent.

Parents should be aware that in such situations they may not be consulted.

In general, the School will assume that pupils consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the School's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the School will maintain confidentiality unless, in the school's opinion, there is a good reason to do otherwise; for example where the School believes disclosure will be in the best interests of the pupil or other pupils.

Pupils are required to respect the personal data and privacy of others, and to comply with the School's Computing and Acceptable Use and E-safety Policies and any School rules.

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2000 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records (as defined in the Education Act).

20. Disclosure of Information

The School may receive requests from third parties to disclose personal data it holds about pupils, their parents or guardians. The School confirms that it will not generally disclose information unless the individual has given their consent or one of the specific exemptions under the Act applies. However the School does intend to disclose such data as is necessary to third parties for the following purposes:

- ✓ To give a confidential reference relating to a pupil to any educational institution which it is proposed that the pupil may attend
- ✓ To give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend
- ✓ To publish the results of public examinations or other achievements of pupils of the School
- ✓ To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of School trips

Where the School receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

21. Information Security

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the general public; files may be seen by the cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

The use of computer passwords is a requirement of the school to avoid unauthorised access. All removable devices e.g. laptops, USB sticks, personal mobile phones and digital cameras must not be used to store School data unless they comply with a School Bring Your Own Device (BYOD) policy, and should be encrypted and pass worded wherever possible.

All members of staff should take care when transporting paper files between sites. No personal data is ever to be left unattended off site e.g. in a car overnight, on view to family members when working at home.

All members of staff should take care when emailing personal data and always check the email address is correct and the right attachment has been attached. When copying to several people externally, all members of staff should always use the BC field and not the CC field or create a group.

22. Maintenance of Up to Date Data

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. In reality most relevant information should be kept for the period during which the person is associated with the School plus an additional period which the School has determined. Under GDPR the School must produce a Retention and Disposal Policy to clarify this.

23. Inaccurate Data

The School will endeavour to ensure that all personal data held in relation to an individual is as up-to-date and accurate as possible. Individuals must notify the DPO of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing.

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. This must be answered within one month. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

24. Recording of Data

Records should be kept in such a way that the individual concerned can inspect them. It should also be borne in mind that at some time in the future the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous, factual and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the School's website will be required to give written consent unless it is a legal requirement (e.g. Governors' details). At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

25. Photographs

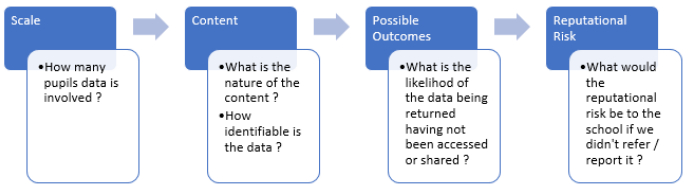
Whether or not a photograph comes under the data protection legislation is a matter of interpretation and quality of the photograph. However, the School takes the matter extremely seriously and seeks to obtain parents' permission for the use of photographs outside the School and, in particular, to record their wishes if they do not want photographs to be taken of their children.

26. Breach of the Policy

Non-compliance with the requirements of data protection legislation by the members of staff could lead to serious action being taken by third parties against the School. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal. It should be noted that an individual can commit a criminal offence under the law, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the data controller.

The school takes seriously any data breach and will, through it's policy and practice endeavour to minimise the risk of a breach. However, in the rare circumstances surrounding a data breach a process will be followed. This process can be seen in Appendix A.

The GDPR states that breaches should be referred to the Information Commissioners Office (ICO) within 72 hours of disclosure. However, it is appropriate for our school to consider the following factors before referring to the ICO :



27. Complaints

Complaints related to the management of data in our school will be handled through our existing Complaints Procedure. Copies of which are available on the school website or from the school office upon request.

28. Requests for Amendments of Data

The GDPR establishes the right to amend any data held that is inaccurate or may have a negative or detrimental effect on an individual. Amendments may take the form of updates, redactions or removals. As a school, we believe that before any amendment request is granted the first step is to view the data so as to ensure that it may be necessary. However, in the rare circumstances surrounding a data amendment request a process will be followed. This process can be seen in Appendix B.

29. Requests for Amendments of Data

The GDPR establishes the right to amend any data held that is inaccurate or may have a negative or detrimental effect on an individual. Amendments may take the form of updates, redactions or removals. As a school, we believe that before any amendment request is granted the first step is to view the data so as to ensure that it may be necessary. However, in the rare circumstances surrounding a data amendment request a process will be followed. This process can be seen in Appendix B.

30. Transparency and Accountability

To ensure that the school is open and transparent about what data it holds and how it will be managed, the school will bear in mind the following prompts in all that it does :

The school will provide every parent with information in relation to their data rights. In addition, it will also provide every new parent with a data statement. This 'statement' will outline the aspects of data that the school will gather and use, as well as stating their purpose, their 'shelf-life' and where it may be shared. Parents will be asked to acknowledge their understanding of this information and accept the reasoning and processing that may occur.

31. School Website

The school will establish a page on its website to ensure that its approaches, policies and practices in relation to data are transparent. It will provide parents with information that may be relevant to their data concerns. It will include :

- ✓ Information about the school's Data Protection Officer (name, contact details etc)
- ✓ Copies of relevant policies
- ✓ Data review and amendment request forms
- ✓ Process flowcharts
- ✓ Step by step guides
- ✓ Complaints policy

32. Introducing A New Initiative or Project

The GDPR requires schools to undertake an evaluation of the data management impact resulting from new initiatives. As a school we will undertake this using our proforma which can be found in Appendix C.

33. The School's Rights To Refuse A Request

The school reserves the right to refuse a request to view or amend data held. This would be rare and only on the following basis :

- ✓ Vexatious requests
- ✓ Where information held maybe required by future legal processes e.g. Child Protection
- ✓ The request would lead to inaccurate and misleading information being recorded
- ✓ The request has come from an individual who has no rights of access

Where the school decides not to adhere to a request it will notify the person who requested of :

- ✓ The reason why the request has been refused
- ✓ Their legal rights of appeal or complaint
- ✓ Their legal rights of referral to the ICO

34. Charges

The school will not usually make a charge in relation to data viewing or amendment requests. However, it reserves the right to do so where the request is proven to be :

- ✓ Vexatious
- ✓ Excessive
- ✓ Unfounded

35. Transitional Period

The introduction of the GDPR has required the school to undertake a significant review of policy and practice in relation to data. Throughout the implementation period, from May 2018 to August 2019, we will keep the implementation under regular review. This will be undertaken by :

- ✓ Termly Data Protection Audits
- ✓ Termly Reports to Governors by the School's DPO
- ✓ An Annual Data Statement

This policy needs to be read alongside the school's data retention and disposal policy.

Appendix 1

Sparkenhoe Parental Data Consent Form

As a school, we are legally required to inform you as to the purpose of any data we hold in relation to you or your child. We must also inform you where we will hold the data, who will have access to it, how long we keep it and when we will delete / destroy it. This relates to any data we hold – whether on paper on our computer systems.

Please be assured that we take every step to ensure the safety of this data.

Below, we have outlined the range of information we expect to hold OR are legally obliged to do so. In each section, we have outlined what we are keeping, where it is kept and what we do with it. We require you as a parent to acknowledge that we have informed you about the data we hold (by signing underneath) each section. By doing so, you are acknowledging that you are happy with the arrangements.

Please note: we will endeavour to inform you in a timely manner of any changes.

Registration Information					
What?	**Probable Content**	**Why?**	**Who?**	**Where?**	**When?**
Registration / Admissions Data	Name D.O.B. Address Telephone contacts emails Medical Issues GP/Dentist Free school meal status Ethnicity / Nationality Languages spoken Religion Previous schools Parental / Carer Details	Legally required to for admission to school Well-being of your child Communication between school and home	All staff (Where necessary) Local Education Authority	Initially completed on paper admission form with parents then entered onto school's information management system Paper Version is filed in the office	Held on file throughout child's time at school Passed onto new school when moving Computer retains copy of records in 'archive'

☐☐I understand the purpose of this data and confirm that I am satisfied with the school's arrangement for managing it

Signed : _____

Tests and Assessment Data					
What?	**Probable Content**	**Why?**	**Who?**	**Where?**	**When?**
Statutory test Results Internal assessments & tests	Foundation Stage Key Stage 1 Key Stage 2 Weekly Assessments (Tests) Phonics Testing	Legally required to provide some data to The Department for Education Monitor progress of children over time. To identify strengths and weaknesses, so teaching can be made more personal	All Staff (Where Necessary) Statutory agencies	Data For the DfE is electronically held Teachers own test results are held in their assessment files (paper) and on an electronic system	Held on file throughout child's time at school + 2 years Passed onto new school when moving On request by Statutory organisation Computer Retains Copy of Records in 'Archive'

☐☐I understand the purpose of this data and confirm that I am satisfied with the school's arrangement for managing it

Signed : _____

CCTV					
What?	**Probable Content**	**Why?**	**Who?**	**Where?**	**When?**
Video recordings of school playground and entrances	All visitors to the school	Security of staff and pupils Reduce insurance claims and costs to the school	Authorised by Headteacher OR Facilities and Premises Manager	The Recordings Are Held Electronically in the School, On The CCTV Master System	Recordings are automatically deleted every 31 days.

☐☐I understand the purpose of this data and confirm that I am satisfied with the school's arrangement for managing it

Signed : _____

Photographs of children				
Probable Content	**Why?**	**Who?**	**Where?**	**When?**
Photographs of children as detailed on admission form	For display and to record school activities. If photos are used in school documents and the school website your child will not be named. Very occasionally photos are taken by outside agencies for example The Leicester Mercury where photos may include a child's name and be used on their website. We may also have TV companies that come and film our children.	Staff Pupils Parents Outside agencies- specific permission will be requested from parent / carers	Displays in school School website Children's workbooks Assemblies Collections of photos for specific events – specific permission will be requested from parents/carers.	School archives will retain some group photographs of events of unnamed children. Digital photos are removed from digital devices as soon as practically possible and saved on the school server Hard copies of photographs are shredded.

I understand that I can inform the school at any time if I wish to withdraw permission for use of my child's photographs.

The School's Data Protection Officer is Mrs P A Cooper, who can be contacted via the school office.

Additional Statement : *Whilst we have endeavoured to outline all the areas in which we gather data, there may well be some additional (short term or specific) requirements. Details related to these can be found on the school website, which will be updated regularly.*

Child's Name : _____

Date of Birth : _____

Name of Person Completing Form : _____

Relationship to Child : _____

Signed : _____ **Date :** _____

Appendix 2 Terms and Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.