Hoyle Court Primary School believes that every child is a learner and can achieve. Our family ethos ensures that everyone is welcomed, respected and valued. We strive to provide citizens of the future who are able to make a significant contribution to the community and to ensure that they are prepared for life in 21st Century Britain.

POLICY TITLE: General Data Protection Regulation (GDPR) Policy & GDPR Privacy Notice		
COMPILED BY: Tim Phillips	DATE APPROVED: 27.4.18	DATE TO BE REVIEWED: 27.4.21

Contents:

Statement of intent

Hoyle Court Primary School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and Hoyle Court Primary School believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

1.3. This policy will be implemented in conjunction with the following other school policies:

- Code of Conduct (staff)
- Freedom of Information Policy

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- The **'Data Controller'** is the School's Governing Body. As the data controller, the Governing Body will implement appropriate security measures that ensure the correct level of protection for all data stored and processed.Complaints can be sent to the data controller if any individual (pupil, staff member or parent) believes that their data has been compromised. If the individual feels that their complaint has not been handled to their satisfaction, they can forward it to the Information Commissioner's Office (ICO).
- The '**Data Processor'** is any person who processes personal data on behalf of the data controller. Under the Data Processing Act, the data controller has an obligation to ensure that data is handled correctly; however, under the GDPR, there will be dual obligations on controllers and processors.

4. Accountability

4.1. Hoyle Court Primary School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2. The school will provide comprehensive, clear and transparent privacy policies.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.5. The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.6. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. The Schools DPO, Adrian Stygall, of 'Safeguarding Monitor' has been appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. An existing employee will only be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

5.4. The DPO will report to the highest level of management at the school, which is the headteacher.

5.5. The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.6. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

6.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.

- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.6. Consent can be withdrawn by the individual at any time.

7.7. For children in school the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

8.2. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time.
  - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

8.3. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

8.4. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

8.5. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.6. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed.

9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. The school will verify the identity of the person making the request before any information is supplied.

9.4. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.7. All fees will be based on the administrative cost of providing the information.

9.8. All requests will be responded to without delay and at the latest, within one month of receipt.

9.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.10. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.11. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

10.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

11.3. The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

11.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.6. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress the school's processing of personal data.

12.2. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3. The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

12.4. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5. The school will inform individuals when a restriction on processing has been lifted.

13. The right to data portability

13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. The school will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

13.9. The school will respond to any requests for portability within one month.

13.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

13.11. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. The right to object

14.1. The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

14.4. Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

14.6. Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

15. Automated decision making and profiling

15.1. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

15.2. The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

15.3. When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

15.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

16. Privacy by design and privacy impact assessments

16.1. The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

16.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

16.3. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

16.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

16.5. A DPIA will be used for more than one project, where necessary.

16.6. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

16.7. The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

16.8. Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

17. Data breaches

17.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

17.2. The headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

17.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

17.4. All notifiable breaches will be reported to the relevant supervisory authority within **72 hours** of the school becoming aware of it.

17.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

17.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

17.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

17.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

17.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

17.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

17.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

18. Data security

18.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

18.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

18.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

18.4. Laptops / PCs will have their screen 'locked' when the owner of the laptop is away from it. This is especially important in a classroom environment and other area which the public (either pupils or parents) may have access.

18.5. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

18.6. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

18.7. All electronic devices are password-protected to protect the information on the device in case of theft.

18.8. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

18.9. Staff and governors will not use their personal laptops or computers for school purposes.

18.10. All necessary members of staff are provided with their own secure login and password.

18.11. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

18.12. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

18.13. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

18.14. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

18.15. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

18.16. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

18.17. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.18. Hoyle Court Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19. Publication of information

19.1. Hoyle Court Primary School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

19.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

19.3. Hoyle Court Primary School will not publish any personal information, including photos, on its website without the permission of the affected individual.

19.4. When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20. CCTV and photography

20.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

20.2. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

20.3. If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

20.4. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

21. Data retention

21.1. Data will not be kept for longer than is necessary. (see Retention of Rerecords Policy)

21.2. Unrequired data will be deleted as soon as practicable.

21.3. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

21.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

22. DBS data

22.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

22.2. Data provided by the DBS will never be duplicated.

22.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Appendix 1

GDPR Privacy Notice for Pupils and Their Families

Introduction

Everybody has a right to have their personal information kept confidential; this includes the children who attend Hoyle Court Primary School and their families. The school is committed to protecting pupils' and families' privacy. These rights are also part of the law, the General Data Protection Regulation which is a European Union regulation that the UK government has decided to keep into the future.

Why does the school have to issue this Privacy Statement?

The school is classed as a Data Processor because the school processes data, for example it shares some attainment data with the Department for Education. Because the school also decides to have some internal systems, such as having systems to make sure the school treats everybody equally, then the school is also a Data Controller. The law requires that we must therefore keep data (personal information) confidential and secure. We must also tell families about what data we keep, why and how we intend to keep it secure.

Why do we keep data?

The School uses data (personal information) for the following main reasons:

- To record who is on the school roll (our admissions)
- To record school attendance
- To assess how well pupils are attaining and to predict how they might attain in the future
- To help keep children safe and healthy (protecting pupils' welfare)
- To make sure that we give equal treatment to all children
- To support the social life of the school community

The school receives most data, works with it, stores it and shares it with others on the legal basis of *Public Task*. This means that these activities are tasks that the school has to carry out.

The school will ask for families for *consent* to our using other data, such as photographs.

Keeping your information private

The school will make every effort to keep your information private. We will lock away paper records and make sure that the computer systems are secure. We will work hard to:

- Prevent any data being lost
- Prevent any data being stolen
- Prevent any data from being deleted inappropriately
- Prevent data being seen by people who have no right to see it
- Prevent data being altered inappropriately

Our laptop computers and other portable devices are protected with passwords and encryption. Any desktop computers that have sensitive information on are also protected with passwords and encryption. Our server is kept secure, the hard disks do not leave the school. The members of staff do not share passwords or leave equipment or paper records in vulnerable places. The school has a robust policy on the use of mobile phones and cameras.

The school receives confirmation from other parties who have access to pupil data (for example a company may help the school to analyse pupil attainment) that they comply with the General Data Protection Regulation.

To help keep children safe it is important that the adults looking after children know if there are any health issues that they have. Although we will share this information, we will only share it with people who need to know it to keep your children safe and healthy.

The school has asked to look after pupils' information. We have also appointed a *Data Protection Officer* who advises and visits the school. He is Mr Stygall who works for a company called Safeguarding Monitor. He has been a head teacher.

The Governing Body has a governor who also looks after pupils' information. Her name is Mrs. Val Sherred.

Families' Data

The sort of data that is personal or sensitive and which should be kept private includes:

- Your family's full name, address and other contact details
- Anything to do with health and welfare
- Anything to do with your religion (if you follow a religion) and your ethnicity
- How your children are getting on in school

The school will ask every family to play their part in protecting other people's personal information (or data) which is why we ask all the children in Key Stage 2 to sign an Acceptable Use Policy. The children and their families have the *right* to have

their data kept confidential and we ask you to share the *duty* to maintain other people's confidentiality.

The school might have to change this notice if there are changes to the law or if the school decides policy changes are needed.

My Child(ren)'s Name(s):

1.) ……

2.) ……

3.) ……

Printed name…….

Signed name……. Dated ……

APPENDIX 2

Data Breach Log (BLANK EXAMPLE)												
Date of breach	**Number of people affected**	**Type of breach**	**Who by?**	**Description of breach**	**How did the school become aware?**	**Who became aware?**	**Date the school became aware**	**Consequences of the breach**	**Action taken**	**Affected people informed**	**Date the breach was raised to the ICO**	**Further training required?**
20/02/2018	4	Lost in transit	Joe Bloggs	Misplaced	When individual who lost data contacted the school	Jane Doe	22/02/2018	Data could be available to numerous individuals	Joe Bloggs given Data Protection Policy	Yes	N/A	Yes

Appendix 3

General Data Protection Regulation GDPR
Privacy Notice for Staff

Introduction

Staff employed by **Hoyle Court Primary School** and contractors engaged by the school have many legal rights regarding how their personal data is obtained, stored, processed and transmitted (i.e. 'processed') both during your period of employment and after. The school has to obtain certain information before a contract of employment may be offered. This privacy notice details how the school will comply with the law and gives you an understanding of why and how the school uses the information about you.

This privacy notice does not form part of your contract of employment. The notice may be updated at any time. All people working with or for the school must comply with this policy when processing data.

The Governing Body and Leadership of Hoyle Court Primary School acknowledge the absolute necessity for correct and lawful treatment of data and are committed to ensuring security for your data.

Roles and Responsibilities

The school is a **Data Controller** as we are responsible for decisions about how and why we use your personal information.

At times the school acts as a **Data Processor** when we are required to obtain, process and transfer data on the behalf of external organisations.

The school has appointed a **Data Protection Officer**

Adrian Stygall, Schools' Liaison Director, Safeguarding Monitor
adrian@safeguardingmonitor.co.uk
0330 400 4142
2 Wellington Place, Leeds, LS1 4AP

Usually the school will coordinate data protection practice through

The Headteacher and School Business Mananger

Mr Stygall may be contracted directly should any employee or contractor feel that their concerns about data protection are not being addressed within the school. Among the DPO's duties are:

- Advice on the secure storage and transmission of data (both physical and digital)
- Updates for the school on the GDPR
- The completion of a data audit
- Support for a data processing record system
- The provision of template GDPR documentation (please note that this cannot be shared beyond the school without the permission of Safeguarding Monitor)
- Reporting to the school's leadership and governing body on levels of security and compliance

- Support with securing certification that they are also complying fully with GDPR duties from third parties who might hold personal data through the school
- The DPO will communicate with the Information Commissioner's Office should there be a confirmed or suspected data breach
- The DPO will communicate with any person whose data might have been improperly accessed, deleted, lost or stolen

The governor who oversees data security for the governing body is: Val Sherred

The principles under which the school will process data

- Data will be kept securely - all employees and contractors share this duty
- Personal information will all be stored no longer than is necessary to exercise the school's duties and statutory requirements
- All employees and contractors will be informed clearly about the purposes for processing data
- Data processing will be limited to the purposes that are explained to employees and contractors
- The school will keep data relevant, current and up-to-date
- The school will only use personal information in a legal and transparent manner

The categories of information and the bases for which that information is processed

In broad terms the school will collect, store, process and transmit data to meet its duties under

- Employment law
- Safer recruitment
- Staff welfare
- Payroll and pension procedures
- Performance Management
- To meet the school's responsibilities under the Equalities Act

Specifically the school will process the following information

Data processed on the legal basis of public task for safe recruitment, promotion and pupil safeguarding

Your application with references, proof of qualification, proof of identity, right to work in the UK, DBS certification, any disability, notes on your recruitment process, your use of IT equipment to ensure compliance with our Acceptable Use Policy and other IT policies

Data processed on the legal basis of public task for employment, payroll and pension procedures and the prevention of fraud

Your data of birth, bank details, payroll details, address, pension choices, national insurance number, a photograph of you, tax status, car details (if you intend to park in the school site), leave entitlement, sick leave monitoring and any disciplinary or capability notes should the need arise

Data processed on the legal basis of public task for staff welfare

Contact details for your next of kin, any medical needs, disability, allergies and any other health needs that you choose to share

Data processed on the legal basis of public task to fulfil the school's duty of accountability

Your performance management, the attainment and achievement of pupils you teach or for whom your share a responsibility, your continuous professional development

Data processed on the legal basis of consent for equality monitoring

You may choose to disclose information regarding your ethnicity, age, religion, gender, sexual orientation and medical needs so that the school can monitor its equality of employment

Data processed on the legal basis of consent to support the school team's social life

With your consent the school use your data to share information about social events organised for the staff

Data processed on the legal basis of consent to support the school's professional relationships

Your trade union membership

This cannot be an exhaustive list, but any further information will be collected and used legally and on either the basis of public task or consent. Much of the information is collected during recruitment and induction. We have to collect some information from former employees and other agencies such as the Data Barring Service. Further information will be collected throughout your period of working for the school. Some information will be processed for external agencies, including future employers on the basis of public task. The principal use of your information will be for the school to perform the contract that applies to our working relationship.

If information required on the basis of the school's public task is withheld then the school might not be able to perform the contract that applies to our working relationship.

You will be notified if we need to use your information in ways other than those so far stated and you will be informed about which legal basis has been selected.

The school regards certain information as particularly sensitive - such as information on physical and mental health, religion, ethnicity and sexuality. Such information will be gathered to support the school's equal opportunities obligations, but will only be gathered given your specific written consent. Such information may also be used to ascertain your fitness to work and to ensure your health and safety and/or to make reasonable adjustments to your working environment and work pattern.

The school does not use your information for automated decision making.

We share some information with third parties most commonly for HR tasks and as required by the law
Payroll and pension, benefits provision and administration

All third parties are required to maintain data security as the law requires.
We require certification from third parties that your information is secure.

After your period of employment with the school we will only keep that information which we are required to do so to fulfil financial, legal and safeguarding duties.

Your duty to inform the school of changes

The school must have up-to-date information which is accurate. Please keep the school informed of any changes to your information while you are employed by the school

Your rights to 'see' your data

Under law, under most circumstances, you have the right to request access to your personal information (usually this is known as a 'data subject request'). Under this right you may request a copy of the information we hold on you and to check that processing is lawful.

You may request correction or completion of any of the data.

You may request that your personal information is erased or restricted if there is information for which there is no good purpose for the school to continue to hold

Please contact the Headteacher in writing should you wish to review, correct or erase personal information, or you may contact the DPO directly. The school has 15 days to meet your request.

Please note that the school has a primary duty of care to the children and may withhold access if it can be demonstrated that this is necessary in the vital interests of a child. You will be informed if this is the case in writing.

There is no fee required for your access to data or for any amendments.

You have the right to withdraw the consent that you have previously granted the school to process certain data. If this is the case then please contact the Headteacher in writing.

School compliance

Hoyle Court Primary School has appointed a Data Protection Officer to oversee compliance with this privacy notice. If you have any questions about your data security or this privacy notice, then please contact the DPO initially.

You have the right to make a complaint to the Information Commissioner's Office (ICO) which is the UK supervisory authority for data protection.

Hoyle Court Primary School may update this privacy notice at any time. A copy of the new notice will be given to you. We may inform you in other ways of any changes that we make to the processing of your data.

I _____ (please print name) acknowledge that I have received and read and understood a copy of **Hoyle Court Primary School** privacy notice.

Signed _____

Dated _____

Appendix 4

General Data Protection Regulation Acceptable Use of IT Agreement for Staff

Introduction

Hoyle Court Primary School commits to protecting the privacy and security of the personal information it holds for staff, governors and volunteers. Please note our Privacy Statements.

To complement the data protection duties of the school there are duties shared by all staff, governors and volunteers because, as a professional organisation with responsibility for children's safeguarding, it is essential that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This agreement covers all digital and physical data systems, e.g. the internet, intranet, network resources, learning platform, software, communications tools (online and offline), equipment (access devices) and paper records, whether printed or handwritten and however stored.

1. I understand that data held by the school may only be processed (acquired, processed, stored, deleted or transmitted) on the legal bases that the school has registered with the Information Commissioner's Office.
2. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation 2018. This means that all personal data will be processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted. Any images or videos of pupils will always take into account parental consent. I will ensure that data no longer needed will be effectively deleted or shredded.
3. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation. Such misuse is also covered by the GDPR and any such misuse must be reported to the ICO, and to the data subjects (people) affected, within 72 hours.
4. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my device as appropriate. I will not use personal equipment to access school data.

5. I will respect system security and I will not disclose any password or security information. I will use a ‘strong’ password. I will adopt school procedures for the safe storage of my passwords and for acquiring new ones.
6. I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). Where possible I will use the School system to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft. I will not share any files or folders on the School system with any other user. I will be mindful that when working in a public space that others may be able to see my laptop, tablet or mobile phone screen and will use my discretion as to whether information should be hidden from site. I am aware that enabling Bluetooth connectivity on mobile devices can be a security threat and will switch this off when it is not needed for a specific connection.
7. I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
8. I will respect copyright and intellectual property rights.
9. I have read and understood the school’s Data Security Policy and e-Safety Policy which cover the security of data and safe and appropriate access to data.
10. I will report all incidents of concern regarding children’s online safety to the Designated Child Safeguarding Lead (Tim Phillips) and/or the e-Safety Coordinator (Ben Dickinson) and/or the lead for Prevent (Tim Phillips) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable/extreme websites to the e-Safety Coordinator.
11. I will not attempt to bypass or alter any filtering and/or security systems put in place by the school.
12. My communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. I will ensure that a BCC of any emails to parents/carers are sent to school/office email address. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
13. I will refrain from using any form of social media to discuss any aspect of school life except purely social events that involve colleagues. I will follow any guidance issued when contributing to the use of social media by the school as an official communication channel.
14. My use of ICT and information systems and my written communication will always be compatible with my professional role whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites or postal addresses. My use of ICT and other forms of communication will not interfere with my work duties and will be in accordance with the school AUP and the Law.
15. I will not create, transmit, display, write, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.
16. I will promote e-Safety (including privacy) with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create. Similarly I will promote care for others in the pupils’ writing and any other content that they create.
17. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

18. The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I _____ (please print name) acknowledge that I have received and read and understood a copy of the Hoyle Court Primary School's Acceptable Use Policy.

Signed _____

Dated _____

Appendix 5

General Data Protection Regulation GDPR
Request for consent for the use of your child's image.

Dear Parent / Carer,

Following the requirements of the General Data Protection Regulation we are writing to families about the use of photographs and videos which might record images of your child.

The school wishes to use photographs for the reasons listed below, but we need your consent (agreement) for this. We are particularly keen that we gain consent for the first purpose listed as we use photographs carefully to support the school's health and safety procedures. This helps us to ensure the best possible standards of pupil welfare.

Your consent will last as long as your child is a pupil at this school, or until you inform us that you want to change your consent.

We will write to you before your child leaves the school should we want to keep or continue to use any photographs of your child after your child leaves the school.

Please can we remind parents that they should follow any guidance at school events about taking photographs or videos? We all need to work together to respect each other's privacy wishes.

I consent to the school using a photograph of my child(ren) to support the school pupil welfare procedures. *Yes* ☐ *No* ☐

I consent to the school using photographs and videos of my child to celebrate achievements in their classroom *Yes* ☐ *No* ☐

I consent to the school using photographs and videos of my child to celebrate achievements in the school *Yes* ☐ *No* ☐

I consent to the school using a photograph of my child to celebrate achievements beyond the school and in the press *Yes* ☐ *No* ☐

I consent to the school using a photograph of my child to celebrate achievements beyond the school and online, and on the school's website

Yes ☐ *No* ☐

My Child(ren)'s Name(s):

1.) ……

2.) ……

3.) ……

Printed name…….

Signed name……. Dated ……