Cottesbrooke Infant & Nursery School
GDPR Policy

Table of Contents

GDPR Policy

1. Purpose

Cottesbrooke Infant & Nursery 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 core principles of the GDPR.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2. Legal Framework

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 Regulations 2004
- The School Standards and Framework Act 1998

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

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation'

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

- Safeguarding Policy
- Freedom of Information Policy
- E-Safety & Acceptable Usage Policy for Staff, Governors & Authorised Visitors

3. Compliance

This policy applies to all governors, staff, authorised visitors and students of Cottesbrooke Infant & Nursery School. Any breach of this policy, or of the Act itself will be considered an offence and the school's disciplinary procedures will be invoked.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

The Information Commissioner's Office (ICO) gives further detailed guidance and Cottesbrooke Infant & Nursery School undertakes to adopt and comply with ICO guidance.

4. Applicable Data

4.1. 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. 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.

4.2. **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.

5. Principles

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

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

5.2. 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.

5.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5.4. 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.

5.5. 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.

5.6. 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 GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

6. Accountability

6.1. Cottesbrooke Infant & Nursery School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

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

6.3. 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.

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

6.4.1. Name and details of the organisation
6.4.2. Purpose(s) of the processing
6.4.3. Description of the categories of individuals and personal data
6.4.4. Retention schedules
6.4.5. Categories of recipients of personal data
6.4.6. Description of technical and organisational security measures

6.4.7. Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

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

6.5.1. Data minimisation
6.5.2. Pseudonymisation
6.5.3. Transparency
6.5.4. Allowing individuals to monitor processing
6.5.5. Continuously creating and improving security features.

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

7. Data protection officer (DPO)

7.1. A DPO will be appointed in order to:

7.1.1. Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.

7.1.2. Monitor the school's compliance with the GDPR and other laws, including:

7.1.2.1. Managing internal data protection activities
7.1.2.2. Advising on data protection impact assessments,
7.1.2.3. Conducting internal audits,
7.1.2.4. Providing the required training to staff members.

7.1.3. An existing governor will 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.

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

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

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

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

8. Lawful processing

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

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

8.2.1. The consent of the data subject has been obtained.

8.2.2. Processing is necessary for:

8.2.2.1. Compliance with a legal obligation.
8.2.2.2. The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
8.2.2.3. For the performance of a contract with the data subject or to take steps to enter into a contract.
8.2.2.4. Protecting the vital interests of a data subject or another person.
8.2.2.5. 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.)

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

8.3.1. Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.

8.3.2. 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.

8.3.3. Processing relates to personal data manifestly made public by the data subject.

8.3.4. Processing is necessary for:

8.3.4.1. Carrying out obligations under employment, social security or social protection law, or a collective agreement.
8.3.4.2. Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
8.3.4.3. The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
8.3.4.4. 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.
8.3.4.5. 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.
8.3.4.6. 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.
8.3.4.7. Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

9. Consent

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

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

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

9.4. 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.

9.5. 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.

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

10. The Right to be Informed

10.1. 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.

10.2. If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

10.3. 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:

10.3.1. The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
10.3.2. The purpose of, and the legal basis for, processing the data.
10.3.3. The legitimate interests of the controller or third party.
10.3.4. Any recipient or categories of recipients of the personal data.
10.3.5. Details of transfers to third countries and the safeguards in place.
10.3.6. The retention period of criteria used to determine the retention period.
10.3.7. The existence of the data subject's rights, including the right to:

10.3.7.1. Withdraw consent at any time.
10.3.7.2. Lodge a complaint with a supervisory authority.
10.3.7.3. The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

10.4. 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.

10.5. 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.

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

10.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:
10.7.1.1. Within one month of having obtained the data.
10.7.1.2. If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.
10.7.1.3. If the data are used to communicate with the individual, at the latest, when the first communication takes place.

11. The Right of Access

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

11.2. 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.

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

11.4. 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.

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

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

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

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

11.9. 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.

11.10. 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.

11.11. 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.

12. The Right to Erasure

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

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

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

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

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

12.4. 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.

12.5. 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.

12.6. 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.

13. The Right to Restrict Processing

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

13.2. 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.

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

- 13.3.1. Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- 13.3.2. Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- 13.3.3. Where processing is unlawful and the individual opposes erasure and requests restriction instead

13.3.4. Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

13.4. 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.

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

14. The Right to Data Portability

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

14.2. 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.

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

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

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

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

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

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

14.8. 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.

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

14.10. 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.

14.11. 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.

15. The Right to Object

15.1. 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.

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

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

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

15.3.1. An individual's grounds for objecting must relate to his or her particular situation.
15.3.2. 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.

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

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

15.5. Where personal data is processed for research purposes:

15.5.1. The individual must have grounds relating to their particular situation in order to exercise their right to object.
15.5.2. 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

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

16. Automated decision making and profiling

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

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

16.2. 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.

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

16.3.1. Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
16.3.2. Using appropriate mathematical or statistical procedures
16.3.3. Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
16.3.4. Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

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

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

17. Privacy by Design and Privacy Impact Assessments (DPIA)

17.1. 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.

17.2. 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.

17.3. 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.

17.4. 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.

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

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

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

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

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

17.8. 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.

18. Data breaches

18.1. 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.

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

18.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed. As per guidance in Appendix D

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

18.5. 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.

18.6. 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.

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

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

18.9. 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.

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

18.10.1. The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
18.10.2. The name and contact details of the DPO

18.10.3. An explanation of the likely consequences of the personal data breach
18.10.4. A description of the proposed measures to be taken to deal with the personal data breach
18.10.5. Where appropriate, a description of the measures taken to mitigate any possible adverse effects

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

19. Data security

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

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

19.3. 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.

19.4. 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.

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

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

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

19.8. Staff will not use their personal laptops or computers for school purposes.

19.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

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

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

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

19.13. 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.

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

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

19.15. 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.

19.16. 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.

19.17. Cottesbrooke Infant & Nursery School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action. The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited. All personal data held

on the school's network is subject to the Data Protection Act 1998 (and subsequently the General Data Protection Regulation (GDPR).

20. Publication of information

20.1. Cottesbrooke Infant & Nursery School publishes on its website Information that will be made routinely available, including:

20.1.1. Policies and procedures
20.1.2. Governing Board Information
20.1.3. Financial information
20.1.4. Operational Updates
20.1.5. Event information
20.1.6. Staff information

20.2. Cottesbrooke Infant & Nursery School will not publish any personal information, including photos, on its website without the permission of the affected individual or his/her parent/guardian.

20.3. 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

21. CCTV and Photography

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

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

21.3. 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.

21.4. Precautions, as outlined in the Safeguarding Policy, are taken when publishing photographs of pupils, in print, video or on the school website.

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

22. Data retention

22.1. Data will not be kept for longer than is necessary.

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

22.3. 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.

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

23. DBS Data

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

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

23.3. 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. 23. Policy review 23.1. This policy is reviewed every three years by the SBM and the Headteacher. The next scheduled review date for this policy is Spring term 2021.

24. Policy review

24.1. This policy is reviewed every year by the Office manager and the Head Teacher.

Appendix A – Staff Privacy Statement

Staff Privacy Notice

The school workforce: those employed to teach, or otherwise engaged to work at, a school or a local authority

The Data Protection Act 1998: How we use your information.

We process personal data relating to those we employ to work at, or otherwise engage to work at Cottesbrooke Infant & Nursery School. This is for employment purposes to assist in the running of the school and to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, NI number, address, contact details
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information
- work absence information (such as number of absences and reasons)
- qualifications
- record of any known disability

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority BCC – Birmingham City Council
- the Department for Education (DfE)

The lawful basis on which we process this information:

We process this information under the Data Protection Act 1998, and according to guidance published by the Information Commissioner's Office and the Department for Education. Under Article 6 of the GDPR, which comes into effect from 25 May 2018, the lawful basis for processing school workforce information is to fulfil contractual obligations and other legitimate interests.

For data collection purposes (Departmental Censuses) provisions of the Education Act 1996 will be followed.

Collecting this information:

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information:

We hold school workforce data throughout your period of employment and for 6 years after the cessation of your employment. Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of documents.

If you require more information about how we and/or DfE store and use your personal data please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Requesting access to your personal data:

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact: Mr Irfan Khan, Data Protection Officer.

You also have the right to:

• object to processing of personal data that is likely to cause, or is causing, damage or distress
• prevent processing for the purpose of direct marketing
• object to decisions being taken by automated means
• in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
• claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns

If you want to see a copy of information about you that we hold, please contact:

Mr William Loughlin
Head Teacher
Cottesbrooke Infant & Nursery School

Appendix B – Parent/Student Privacy Statement

Privacy Notice (How we use pupil information)

Why do we collect and use pupil information?

Cottesbrooke Infant & Nursery School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, LA and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard pupils

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- SEND pupil information
- Pupil assessment and attainment data
- Medical information
- Behaviour information
- Safeguarding information

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

Personal data relating to pupils at Cottesbrooke Infant & Nursery School and their families is stored in line with the school's GDPR Data Protection Policy. In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected. The table below shows for how long we keep different types of information about your child.

Type of Information	Retention Period, or the criteria used to determine the retention period
Parent correspondence and financial details	Six years after pupil has left school
Parent correspondence details (nonstarter)	Five years after completion of paperwork
Pupil acceptance details	Six years after pupil has left the School
Pupil records	Transferred securely to the next School/ any records retained Six years after pupil has left the School

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- School Nurse
- SEND External Support e.g PSS, BSS, Educational Psychologist
- SENAR

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mr Khan (Data Protection Officer) or Mr Loughlin (Head Teacher)

You also have the right to:

- be informed about how Cottesbrooke Infant & Nursery School uses your personal data
- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means

- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time. If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact:

- Mr Irfan Khan – Data Protection Officer at Cottesbrooke Infant & Nursery School.
  or
- Mr William Loughlin – Headteacher at Cottesbrooke Infant & Nursery School

Appendix C – E-Safety & Acceptable Usage Policy for Staff / Governors / Authorised Visitors

Cottesbrooke Infant & Nursery School
E-Safety & Acceptable Usage Policy for Staff / Governors / Authorised Visitors

(May 2018)

1. Introduction

1.1. The governing body of Cottesbrooke Infant & Nursery School has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital mobile devices.

1.2. This E-Safety Acceptable Usage Policy covers the security and use of ALL Cottesbrooke Infant & Nursery School's data and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all users who have control over, or who use, or support the school's IT systems or data including employees, governors, contractors and authorised visitors

1.3. The policy was adopted by the governing body on 04-05-2018 and will be reviews annually in the light of guidance from the local authority or earlier if the local authority issues further guidance in the light of particular circumstances or developments in information and communication technology.

2. Purpose

This Policy is aimed at encouraging responsible behaviour and good practice. It has been created with the view to:

2.1 Ensure compliance and enforcement of relevant legislation which include but is not limited to:

- GDPR (General Data Protection Regulations)
- Computer Misuse Act 1990
- Copyright, Design & Parents Act 1988

2.2 Ensure the safety and integrity of students, staff and members of the school community;

2.3 Prevent damage to the school and its physical/intellectual property.

3. Basic Principles

3.1. In adopting this policy the governing body has taken into account the expectation by Ofsted that rigorous e-safety policies and procedures are in place in the school, written in plain English, with contributions from the whole school, updated regularly and ratified by governors.

3.2. This policy applies to all members of the school community, including staff, pupils, volunteers, parents and carer's, governors, visitors and community users who have access to, and are users of, the school's information and communication technology systems or who use their personal devices in relation to their work in school.

3.3. The governing body expects the head teacher to ensure that this policy is implemented, that training in e-safety is given high priority across the school, that consultations on the details of the arrangements for e-safety continue with all employee on a regular basis, and that any necessary amendments to this policy are submitted to this governing body for approval.

3.4. The principle context for this policy is the need to safeguard children. It will be applied in conjunction with the school's behaviour and anti-bullying policies for pupils and with the rules and procedures governing the conduct of employees.

3.5. The governing body expects the head teacher to arrange for this policy to be published to all employees and volunteers in the school and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

4. Roles and Responsibilities

Governing Body

4.1. The governing body will consider and ratify this e-safety policy, and review it annually in the light of guidance from the local authority, or sooner if the local authority issues new guidance in the light of particular circumstances or developments in information and communication technology. Governors are expected to follow the policy in the same way as the rest of the school community are expected to follow it, including:

- Signing an E-Safety & Acceptable Usage Policy (AUP) which sets out basic rules of IT safety and focuses on E-safety.
- Signed an acceptance of the School's Data Protection Policies.
- Participating in E-safety training if they use information and communication technology in their capacity as school governors.

4.2. Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that Birmingham City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head teacher

4.3. The head teacher is responsible for ensuring that:

- The governing body is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils' behaviour, take account of this e-safety policy;
- The governing body is given necessary advice on securing appropriate information technology systems;
- The school obtains and follows Birmingham City Council or other reputable guidance on information technology to support this policy;
- The school has a designated senior person to co-ordinate e-safety and that this person has adequate support from, and provides support to, other employees, particularly the designated senior person for safeguarding;
- There is effective consultation with all employees, and other users of the school's information and communication technology systems, to take account of the particular features of those systems and educational , technical and administrative needs;
- The school provides all employees with training in e-safety relevant to their roles and responsibilities and that training is also provided to volunteers and school governors who use information and communication technology in their capacity as volunteers or governors as the case may be;
- The senior leadership team is aware of the procedures to be followed in the event of a Data Breach (GDPR Policy – Section 18 & Appendix D)
- Pupils are taught e-safety as an essential part of the curriculum;
- The senior leadership team is aware of the procedures to be followed in the event of a serious e-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem;
- Records are kept of all e-safety incidents and that these are reported to the senior leadership team
- Necessary steps have been taken to protect the technical infrastructure and meet the technical requirements of the school's information and communication technology systems
- There is appropriate supervision of, and support for, technical staff;
- Any outside contractor which manages information technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

Other Employees

4.4. Other employees responsible for:

- Undertaking such responsibilities as have been delegated by the head teacher commensurate with their salary grade and job descriptions;
- Participating in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- Using information and communication technology in accordance with this policy and the training provided;
- Reporting any suspected misuse, breach or problem to the person designated by the school for this purpose.

Pupils

4.5. Pupils are expected to use information and communication technology systems and devices as they have been taught in accordance with the school's behaviour policy and the instructions given to them by staff

Other Users

4.6. Volunteers who help in the school and who use information and communication technology systems and devices in helping the school are expected to:

- Accept and sign an E-Safety & Acceptable Usage Policy (AUP) which sets out basic rules of IT safety and focuses on E-safety.
- Sign an acceptance of the School's Data Protection Policies.
- Participate in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- Use information and communication technology in accordance with this policy and the training provided;
- Report any suspected misuse or problem to the person designated by the school for this purpose.

Parents

4.7. Parents who help in the school as volunteers are covered by **4.6** above. Parents who are not voluntary helpers in school are nonetheless subject to the law in the event of misuse of information and communication technology.

I.T Department

4.8. The ICT Operations Manager is responsible for the smooth operational running of the School's IT equipment, software, network infrastructure and of IT security.

The ICT Operations Manager must manage access rights to systems granted to an individual user. Access rights are recorded in Active Directory and in CMIS.

A record of changes to the rights (amended or withdrawn) resulting from a change to responsibilities or termination of employment must be recorded in Active Directory.
All access rights are removed in a timely manner when an individual's employment is terminated.
The IT department must manage IT assets (via an inventory) and allocation of IT equipment including the return of IT equipment when a member of staff leaves the School.

5. Acceptable Use

5.1. The use of information and communications technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's information and communication technology systems are intended primarily for educational use and the management and administration of the school. During work breaks appropriate, reasonable personal use is permitted.
- GDPR and other related legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.
- Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the school.

5.2. Employees, volunteers and governors should:

- Only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians;
- When recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
- Communicate with pupils, parents, governors, contractors and authorised visitors only through the school's official communication systems
- Report any damage or faults to the appropriate member of staff.
- Ensure that their data is backed-up regularly via encrypted hardware or authorised cloud storage. The use of unencrypted storage devices is prohibited.

5.3. Employees, volunteers and governors must NOT:

- Allow anyone else to use their UserID/password on any school IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's UserID/password to access the school's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to the school's IT systems or information.
- Attempt to access data that they are not authorised to use or access
- Connect any unauthorised device to the schools network or IT systems.
- Install unauthorised software on the school systems.
- Leave any devices exposed or unattended outside the school premises.
- Access, copy, remove or alter any other user's files without that person's express permission
- Use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
- Use personal social networking sites through the school's information and communication technology systems. Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally. The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute
- Open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted;
- Deliberately disable or damage any information and communication technology equipment;
- Share, without authorisation, schools data/information that is classed as 'personal' or 'sensitive personal' data as per GDPR legislation.
- Transport, copy or move data/information from the school systems via unsecure methods. The use of unencrypted storage devices is prohibited.

5.4. Electronic mail (e-mail)

5.4.1. Members of staff and members of the governing body will be provided with email services for school related communication.
5.4.2. Caution should be exercised when sending confidential information via e-mail.
5.4.3. Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
5.4.4. The transmission of confidential information to unauthorised persons, or using the schools email system for personal business is strictly prohibited.
5.4.5. While Cottesbrooke Infant & Nursery School respects the privacy of staff, members of the governing body and authorised visitors, the school reserves the right to monitor and intercept e-mail communication.
5.4.6. Any e-mail communication made must not bring the School into disrepute; this includes anything libellous, defamatory or criminal.
5.4.7. If a staff member is not sure that an email they received is safe, they must refer to the IT Manager, and should never forward suspicious emails.

5.5. Internet Access

5.5.1. Cottesbrooke Infant & Nursery School will only provide access to the Internet on receipt of a signed Policy.
5.5.2. All Internet access is monitored for the purposes of maintaining standards of security and acceptable use.
5.5.3. Attempts to access inappropriate websites or websites which attempt to bypass filtering systems constitute a breach of this Acceptable Use Policy.
5.5.4. Inappropriate websites referred to in **5.5.3** include, but are not limited to any site which contains:

- Pornographic Material (of either a legal or illegal nature);
- Material which incites hatred or discrimination;
- Material which promotes illegal activity;
- Material which is in breach of the Copyright Designs and Patents Act 1998;
- Material which is degrading to persons or groups of;

5.4.5 Staff, members of the governing body and authorised visitors are required to report any website that they become aware of, which is not filtered, that is deemed inappropriate as per the criteria stated within **5.5.4.**
5.4.6 While Cottesbrooke Infant & Nursery School, in conjunction with Birmingham City Council, uses sophisticated filtering technology and takes all precautious to ensure that users only access appropriate material, it is not possible to guarantee that unsuitable material will be inaccessible. Neither the School nor Birmingham City Council can accept liability for the material accessed, or any consequences of such access.

5.5 Network Access

5.5.2 Staff, members of the governing body and authorised visitor logins must only be used by the member of the school community that they are issued to. Liability remains with the logged in user.
5.5.3 Allowing another person to use your login is a severe breach of this Acceptable Use Policy and contravenes legislation.
5.5.4 Passwords must never be divulged to anyone at any time.
5.5.5 If it is suspected that a password has been compromised it must be changed immediately.
5.5.6 If you leave your computer unattended, either log out or lock it by using the ‘CTRL ALT Delete’ keys and then choosing “Lock Workstation”. Once this is done, you will need to re-enter your password to gain access to the computer
5.5.7 Staff, members of the governing body or authorised visitors will not attempt to download or install software onto the network or IT Equipment, including allocated laptops.
5.5.8 It is prohibited to copy any software or inappropriate material on to the network.
5.5.9 Staff, members of the governing body or authorised visitors will not store confidential material on network areas which are accessible to persons who do not have clearance to access such material.
5.5.10 Staff, members of the governing body and authorised visitors understand that the right is reserved to remotely monitor and intercept network activity.

5.6. Transfer data securely

Transferring data introduces a security risk. Staff must:

5.6.1.1. Avoid transferring sensitive data (e.g. pupil information, reports or marking sheets) to other devices or accounts unless absolutely necessary
5.6.1.2. Only share sensitive data over the Schools network/ system, the schools OneDrive cloud storage or encrypted storage devices and not over public Wi-Fi, unencrypted storage or private connection.
5.6.1.3. Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
5.6.1.4. Ensure any email attachments containing data are password protected
5.6.1.5. Report scams, privacy breaches and hacking attempts.

5.7. ICT Equipment and Suites

5.7.1. Staff, members of the governing body or authorised visitors may not move or authorise any person to move any installed ICT Equipment.
5.7.2. Staff, members of the governing body or authorised visitors may not pass on any ICT Equipment to any other person. It must first be passed back to the ICT department and then reissued.
5.7.3. Any equipment issued to staff, members of the governing body or authorised Visitors remains the property of the school and must be returned upon request.
5.7.4. Upon termination of employment at the School all equipment must be returned.
5.7.5. Staff, members of the governing body and authorised visitors are responsible for all equipment issued to them and must take reasonable precautions to protect such equipment including securing equipment at all times.
5.7.6. Equipment taken off-site is not insured by the school. If any school ICT equipment (including loaned laptops) is/are taken off-site, it should be ensured that adequate insurance cover has been arranged to cover against loss, damage or theft.
5.7.7. Staff are responsible for all equipment and use of workstations by students during their lessons in ICT Suites.
5.7.8. Staff, members of the governing body and authorised visitors must ensure that ICT Suites are secured upon leaving the room.
5.7.9. No students may be allowed to use ICT Suites without suitable supervision by a member of staff, member of the governing body or an authorised visitor.

5.8. Mobile Phones & Personal Digital Devices

5.8.1. Staff, members of the governing body and authorised visitors use of personal mobile devices during their working school day should be:

5.8.1.1. Outside of their contracted / agreed hours
5.8.1.2. During allocated break and dinner times
5.8.1.3. Discreet and appropriate e.g. Not in the presence of pupils

5.8.2. Mobile devices should be switched off and left in a safe place during lesson times. There are lockers available in the staff room. The school will not take responsibility for items that are lost or stolen.
5.8.3. Staff, members of the governing body and authorised visitors should never contact pupils or parents from their personal mobile phone, or give their mobile phone number to pupils or parents. If a member of staff, member of the governing body or authorised visitor needs to make telephone contact with a pupil or parent, a school telephone should be used.
5.8.4. Staff, members of the governing body and authorised visitors should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate.
5.8.5. With regard to camera mobile phones, members of staff, members of the governing body and authorised visitors should never use their personal mobile device to photograph a pupil(s), or allow themselves to be photographed by a pupil(s).
5.8.6. Staff, members of the governing body and authorised visitors should be aware that when on outings or trips they must not use their personal mobile device to take photos of children.

5.8.7. In the event that a member of staff, members of the governing body or an authorised visitor has a particular reason for a specified period of time, they may request, via the Head teacher that they leave their phone on during working hours.

This guidance should be seen as a safeguard for staff, the school and the whole school community. Members of staff, members of the governing body and authorised visitors should understand that failure to comply with the policy is likely to result in the enforcement of our Whistleblowing policy and associated procedures.

5.9. Additional Systems

5.9.1. Members of staff may have access to additional systems which include, but are not limited to: CMIS, CPOMS, Target Tracker and CRISP.
5.9.2. These systems require additional passwords. It is the responsibility of the member of staff to ensure that their password has basic complexity to it and that their password is only known by them.
5.9.3. If you leave your computer unattended, either log out or lock it by using the 'CTRL ALT Delete' keys and then choosing "Lock Workstation". Once this is done, you will need to re-enter your password to gain access to the computer

5.10. Encrypted Storage Devices

5.10.1. Personal data in electronic form must only be removed/copied from the school network using authorised cloud storage (Office365-OneDrive) or a school provided encrypted USB memory key
5.10.2. The use of other electronic data storage devices such as iPods, MP3 Players, FireWire devices, non-encrypted USB memory keys and others, to remove personal data from school premises is not permitted.
5.10.3. Care must be taken to ensure that any personal data removed from the school (whether on laptop, Encrypted USB memory key or in paper form) is kept secure from theft and viewing by unauthorised persons.
5.10.4. Any computerised personal data removed from the school must be deleted from any device immediately work is complete.

6. Education and training

6.1. Education and training in e-safety will be given high priority across the school.
6.2. The education of pupils in e-safety is an essential part of the school's e-safety provision and will be included in all parts of the curriculum.
6.3. The school will offer education and information to parents, carers and community users of the school about e-safety.
6.4. Suitable training will be provided through the school for all employees, as part of induction and subsequently during their employment in the school. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and data protection. It will cover related matters such as the law on copyright of electronic materials.
6.5. Volunteers and governors who use information and communication technology during their work will be offered the same training as employees.

7. Data Protection

7.1. The school will ensure that its information and communication technology systems are used in compliance with current data protection legislation and that all users are made aware of the school's data protection policy, including the requirement for secure storage of information.

8. Technical aspects of e-safety

8.1. The school will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems.
8.2. The school will undertake regular reviews of the safety and security of its information and communication technology systems.

8.3. Particular attention will be paid to secure password protection and encryption for devices located in the school and mobile devices.

8.4. The school's systems will also provide for filtering internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.

8.5. The school will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as 'spam'). It should safeguard children and adults against inappropriate use. It should provide the head teacher and senior leadership team with regular reports to indicate whether or not there have been any incidents.

8.6. Additional monitoring may take place as part of an investigation following evidence of apparent misuse.

9. Dealing with incidents

9.1. Any suspicions of misuse or inappropriate activity related to child protection should be reported as prescribed in the Safeguarding Board's child protection procedures.

9.2. Any suspicions of other illegal activity should be reported to the head teacher, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police and may also instigate disciplinary procedures.

9.3. Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the head teacher or other designated member of the senior leadership team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the school's behaviour policy for pupils.

10. Legislation

10.1. All network users are bound by current relevant legislation. The applicable laws (as amended) include, but are not limited to:

- GDPR 2018 (General Data Protection Regulation)
- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1998
- Criminal Justice Act 1988
- Defamation Acts 1952 and 1996
- Freedom of Information Act 2000
- Human Rights Act 1998
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1988
- Protection from Harassment Act 1997
- Public Order Act 1986
- Race Relations Amendment Act 2000
- Telecommunications Act 1984
- Data Protection Acts 1994 and 1998
- Sex Discrimination Act 1986
- Regulation of Investigatory Powers Act (RIPA) 2000

10.2 Staff, members of the governing body and authorised visitors should understand that any attempt to bypass the School, or other network security systems, including the introduction of viruses or applications of a destructive nature could lead to prosecution.

10.3 Where it is believed that a member of staff, member of the governing body or an authorised visitor is in breach of legislation appropriate action will be taken.

11 Sanctions

11.1 In the event that this E-Safety / Acceptable Use Policy is breached, the responsible person(s) will be subject to sanctions which may include, but are not limited to:

- Disciplinary procedures;
- Temporary or permanent restriction of network access;
- Temporary or permanent revocation of network rights;
- Restriction to or denial of access to ICT Suites;
- Investigation under the Regulation of Investigatory Powers Act (RIPA) 2000.

12 Policy Statement

12.1 Cottesbrooke Infant & Nursery School reserves the right to amend this Policy, at any time, without notice. It is your responsibility to ensure that you are up to date with such changes.

12.2 This Policy replaces and supersedes all previous versions, including the 'Staff E-Safety Code of Conduct' policy.

User Agreement

I have read and understood the 'E-Safety & Acceptable Usage Policy for Staff / Governors / Visitors policy for Cottesbrooke Infant & Nursery School.

I understand that should I be found in breach of the Acceptable Use Policy I may be liable to disciplinary procedures and, if appropriate, the Police and local authorities may become involved.

I accept that it is my responsibility to be aware of amendments to this Acceptable Use Policy which can be found on the School's Intranet under the E-Safety section.

Staff Name *		*** USE BLOCK CAPITALS**	
Staff Signature		**Date**	DD / MM / YY

School Agreement

I acknowledge the above named member of staff with has returned a signed Acceptable Use Policy which signifies agreement to all clauses of the Acceptable Use Policy.

I therefore grant access to the network from the date below and permit access to the School's ICT Resources under the conditions of this Policy.

Staff Name *		*** USE BLOCK CAPITALS**	
Authorised Signature		**Date**	DD / MM / YY
Position *		*** USE BLOCK CAPITALS**	

Appendix D – Data Breach Flowchart