Guardian Angels Catholic

Primary School

DATA PROTECTION POLICY

Written By	A Spindlow
Date Agreed	March 2018
Chair of Governors (Signature)	
Head Teacher (Signature)	Mrs Mary Johnson (Interim)
Date for review	March 2019
Links to Other Policies	Safeguarding and Child Protection Policy Freedom of Information Online Safety Policy Use of Images Guidance
Rights Respecting Links	

1. Purpose

1.1. This policy sets out how all staff and governors at Guardian Angels Catholic Primary School ensure that personal information[1] is dealt with correctly and securely and in accordance with relevant Data Protection law, including the General Data Protection Regulations (GDPR), as well as related UK Data Protection legislation.

1.2. This policy should be read in conjunction with *Freedom to Information Policy, Records Management Policy, CCTV Policy, Use of Images Policy, Safeguarding Policy*

2. Data Protection Law

2.1. The GDPR provides a framework for how organisations use personal information. It protects and enforces the privacy of personal information whilst also allowing for the lawful and appropriate use of this type of information about pupils, staff, parents and others who have contact with the School.

2.2. The Law applies to many types of organisation processing personal information, including Schools. It covers all personal information regardless of its format or the way it is collected, used, recorded, updated, stored and destroyed.

2.3. Personal information relates to an individual who can be identified by that information or along with other information likely to come into a person's possession. The School acknowledges that the definition also covers opinions about an individual, information regarding the intentions of the school towards them, and more sensitive 'Special Categories'[2] of information.

2.4. The GDPR is underpinned by a set of six straightforward principles; the School is committed to following these principles as set out in this policy.

3. Processed Lawfully, Fairly and Transparently

3.1. The School will inform pupils, staff, parents and any other person why they need their personal information, how it will be used, with whom it may be shared and anything else required. This will be done via clear and easy to understand statements on forms and Fair Processing Notice documents issued when collecting information or as soon as possible afterwards; they will also be published on the School website where relevant.

3.2. For the majority of personal information the School's lawful basis for processing it is necessary for compliance with a legal obligation. Where this is not the case, consent to use personal information will be sought from individuals.

3.3. Where necessary, the School will conduct Privacy Impact Assessments to ensure the processing of information by the school does not pose a risk to the rights and freedoms of pupils, staff, parents and any other data subjects.

4. Collected for Specified, Explicit and Legitimate Purposes

4.1. Personal information collected and held for the purposes we have stated will not be used for any other purpose without first informing those individuals whose information it is.

4.2. In accordance with UK law the School is registered as a Data Controller with the Information Commissioner's Office and will renew this annually.

---

[1] Inclusive of more sensitive personal information known as 'Special Categories' under the General Data Protection Regulations

[2] This includes more sensitive information and includes information about an person's race, ethnic origin, political opinion, religious and philosophical beliefs, trade union membership, genetics and biometrics, their health, sex life and sexual orientation.

5. Adequate, Relevant and Necessary

5.1. The School will only collect and store personal information that is sufficient for the purpose we have stated and will not ask for more information than is necessary.

5.2. The School will regularly review its forms and will check personal information already held for missing, irrelevant or seemingly excessive information.

6. Accuracy

6.1. Information held by the School will be as accurate and up to date as is reasonably possible and steps will be taken to regularly check the accuracy of personal information held; an example is the annual data collection form issued to all parents to check details are up-to-date.

6.2. If a pupil, member of staff, a parent or any other person informs the School of a change of circumstances or an error in their personal information it will be reviewed and updated as soon as is practicable.

7. Retention of Information

7.1. The School will not keep personal information for longer than is necessary for the stated purpose(s). In order to ensure this, all information held and/or created by the School or held on its behalf will be retained according to timescales set out in the Retention Schedule created by *the Information and Records Management Society (IRMS), and located in our school Records Management Policy.*

7.2. The School will ensure that all personal information deleted or physically destroyed is done in a secure and confidential way.

8. Access

8.1. The School acknowledges that the Law gives specific rights[3] to any person whose details are processed by the School, and will ensure these rights can be exercised where relevant.

8.2. These rights include the right to access information held about them.[4] The School will ensure clear procedures are in place to allow for this and will supply the information sought within the required timescale of one calendar month from date of written request.

8.3. Where a pupil is under the age of 13 years old or it is clear a pupil does not understand the nature of data protection, a written request from parents/carers in respect of their own child will be processed as requests made on behalf of the child and the copy will be supplied to the parents/carers.

8.4. The right to access information held about them applies equally to staff and any other individuals for whom the school holds information about.

8.5. Any third party information (information about someone other than the requesting individual) found will generally be removed or redacted unless third party permission to disclose is provided or it is reasonable in all circumstances to disclose it.

8.6. The School also acknowledges that the Education Regulations 2005 give rights to parents/guardians to their child's *educational* record. The School will respond to such requests **within 15 School days**.

[3] Under GDPR these are the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; rights in relation to automated decision making and profiling

[4] There are a few exceptions to this rule, but most individuals will be able to have a copy of the information held on them

9. Appropriate Security

9.1. To prevent unauthorised or unlawful processing and to protect against accidental loss, destruction or damage to personal information, the School will ensure adequate security measures are in place to safeguard all personal information whether held in paper files, on a computer system, laptop/tablet or on portable media storage devices[5].

9.2. Paper records and portable devices are locked away when not in use and are only accessed by those authorised to see the information held on them. Personal information held electronically is kept securely, is protected by passwords, and is only accessed by those authorised to see the information held.

9.3. Where it is necessary to store or transport personal information on a portable device such as a laptop/tablet or other storage device the relevant equipment or portable media will always be encrypted.

9.4. The School will ensure that staff are aware of the additional precautions they should take when taking personal information, in any format, outside of school for training, meetings or to work from home, such as only taking what is needed, protecting it in transit, never leaving it unattended and storing it securely.

9.5. Particular care will be taken by all staff when sending personal information via emails, faxes and letters, etc. to use secure methods where necessary and to confirm addresses/numbers beforehand.

9.6. The School will undertake a regular review of measures in place to protect personal information taking into consideration developments in technology and ensuring staff receive up to date training and guidance.

10.1 Using Data Processors

10.1. The School will ensure that any third parties who process personal information on the School's behalf will do so under strict written instruction that is binding on the third party, who will also have adequate safeguards in place to protect the information.

10.2. Records of checks of adequate security and the written instruction will be maintained by the School for reference and regular review.

11. Transfers outside of Europe

11.1. Data Protection law applies to all member states within the EU and the UK. The School is unlikely to transfer any personal information outside of the UK and Europe, however, if this is necessary, checks will be made to ensure an adequate level of protection for that information and consent will be sought from those affected if necessary.

12. School Specific Issues

12.1. Consent

12.1.1. The School will seek consent/parental consent to use certain types of personal information where appropriate. Examples of when the School will seek consent include using photographs or recordings of children in school for school projects or for display; using photographs of children, staff and parents in school publications such as newsletters; using photographs of children, staff and parents in external publications such as a local newspaper; using photographs/recordings of children, staff and parents to be on any web page or social media site.

12.1.2. When collecting consent the School will provide a clear explanation of the use of the information and will ask for a positive written indication of consent for each different use. Consent will not be inferred from a non-response to

[5] E.g. USB Memory Sticks, CD's, external hard drives, etc

communication, for example from a parent's failure to return or respond to a letter.

12.2. CCTV

The School utilises CCTV for security and safety purposes. CCTV footage will feature personal information; therefore the School ensures access to the footage and equipment is restricted and makes sure that pupils, staff, parents and visitors to School premises are aware that CCTV is in use by displaying clear signage in and around School premises.

12.3. Public Displays

If there is a display of pupils' work to be shown at a public venue, (other than the school premises), parents will be informed and unless they have consent to publish fuller information, the School will only include the minimum of pupil identifiable information, for example "by John, Year 1".

12.4. School Plays

Data Protection law does not prevent parents/guardians from capturing their child's performance on camera or video as these instances would be for personal/family use only and therefore Data Protection law does not apply. *However any images captured of children that are not their own will not be shared on Social Media as stated in our Social media Policy.*

13. Complaints

13.1. Complaints will be dealt with in accordance with the School's complaints policy. Complaints relating to information handling may also be made to the Information Commissioner's Office (the statutory authority).

14. Contacts

14.1. If you have any enquires in relation to this policy, please contact *Guardian angels school on enquiry@grdangel.bham.sch.uk*, who will also act as the contact point for any access requests.

15. Review

15.1. This policy will be reviewed and updated as necessary to reflect best practice or amendments made to Data Protection law.

Appendix 1: Personal data breach procedure

This procedure is based on **guidance on personal data breaches** produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via **the 'report a breach' page of the ICO website** within 72 hours. As required, the DPO will set out:

1. A description of the nature of the personal data breach including, where possible:
2. The categories and approximate number of individuals concerned.
3. The categories and approximate number of personal data records concerned

4. The name and contact details of the DPO
5. A description of the likely consequences of the personal data breach
6. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible