FARNEY CLOSE SCHOOL

Data Protection Policy

Date Published	**October 2020**
Reviewed	**September 2022**
Review Due	**September 2024**

Approval Level	☑ **Governing Body** ☐ **Principal to Determine**
Signed	
Role	
Date Approved	

Data Protection Policy

1. Purpose

This policy sets out the processes and procedures for ensuring that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations 2018, other relevant legislation, and best practice.

The principles set out within this policy apply to personal information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

2. Scope

This policy applies to all employees and volunteers of Farney Close School who access or use personal data that Farney Close School is responsible for as Data Controller.

This policy should be read in conjunction with the following other Farney Close School policies; Safe Recruitment Policy, Whistleblowing Policy, Safeguarding Policy, Acceptable Use of Technologies Policy, and Data Protection Policy.

This policy doesn't form part of any contract of employment and may be amended from time to time.

3. Schedule of Responsibilities

Farney Close School's Governing Body will ratify this policy.

The Principal works in conjunction to monitor information handling at Farney Close School and ensuring compliance with the law, guidance and local procedures including responding to requests for personal data.

The Principal will take active steps to promote good practice under this policy, monitor and review the management and implementation of this policy at Farney Close. The School Data Protection Lead who will take responsibility for data protection within this setting. The Principal, alongside the Data Protection Lead will identify training needs, ensuring competence of all staff and volunteers as they are responsible for the operation of this policy.

All employees are required to cooperate fully and positively with the requirements of the Data Protection Policy, know the standards of conduct and behaviour expected of them and seek clarification if unsure. All staff are expected to undertake any training recommended by their line manager; ensuring efficient and competent operation of this policy.

All employees are required to bring to the attention of a senior member of staff any loss of data or concerns relating to confidentiality and data protection.

4. Introduction

Farney Close School collects and uses personal information about other individuals who they come into contact with. This information is processed in order to enable the school to provide education and care, and other associated functions, including legal requirements or statutory obligations. Subsequently, in the course of

their work, Farney Close staff will have access to large amounts of confidential and personal information, including but not limited to information about young people, staff members and others.

Farney Close is responsible for the activities in the school and is therefore the legal entity responsible for the processing of personal data by the school.

In accordance with the duty to notify the Information Commissioners Office (ICO) that we process personal information, and to maintain an up to date Registration with the ICO of how and why we process personal data, Farney Closes' registration number is **Z8259549.** A copy of the notification document is available to view at Farney Close, and on ICO's website by following the link https://ico.org.uk/esdwebpages/search. Farney Close will ensure that the registration is renewed annually and that the registration fee is paid.

5. The General Data Protection Regulations 2018

GDPR replaces the Data Protection Act 1998. This new act covers the collecting and holding of information about an identifiable living individual, and its use, disclosure, retention and destruction. It gives people the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly. For further information, see 'Guide to data protection' on the website of the Information Commissioners Office https://ico.org.uk/fororganisations/guide-to-data-protection/

Personal data means information about a living individual who can be identified from that information and from other information, which is in, or likely to come into, Farney Closes' possession.

GDPR defines 'sensitive personal data' as that related to racial or ethnic origin, political opinions or religious beliefs, trade union membership, physical or mental health condition, sexual life, and convictions, proceedings and criminal acts.

The holding of sensitive personal information generally requires the explicit consent of the person; where the request received relates to a child or young person, Farney Close normally obtains this consent from children or young peoples' parents/guardians in writing as part of its needs assessment. For young people over the age of 14 this permission is sought from them. Where the person lacks the capacity to consent and has no representative that can give consent, a best interests decision will be made by Farney Close.

GDPR works in two ways. Firstly, it states that anyone who processes personal information must comply with principles that data should 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.

Secondly it specifies that the data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

6. Policy Principles

Farney Close will take all practical steps to ensure that the requirements of the GDPR 2018 are achieved and maintained throughout the organisation at all times.

Farney Close School will:

- Demonstrate compliance with the GDPR through a range of accountability measures including; Privacy Impact Assessments, Annual Data Audits, Annual Policy Review and the appointment of a dedicated Data Protection Officer.
- Will publish Privacy Notices informing why data is being collected at the point it is collected, including the legal grounds for collection.
- Will seek consent for the processing of personal data.
- Create, maintain and publish a Disposal and Retention Schedule setting out retention and disposal dates for common data sets and other information.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests (see section 15)
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Adopt internal procedures for detecting, reporting and investigating a personal data breach.
- Ensure that processes for handling personal information are only available to authorised individuals.
- Share information with others only when it is legally appropriate to do so, utilising Information Sharing Agreements in accordance with the ICO's Data Sharing Code of Practice, where necessary.
- Share personal data with the police or others for the purpose of crime preventions and detection, the apprehension or prosecution of offenders or for the purpose of legal proceedings, where properly requested.
- Ensure our staff are appropriately trained and aware of and understand our policies and procedures.

7. Privacy Impact Assessments

Privacy Impact Assessments will be carried out when planning new initiatives which involve "high risk" data processing activities i.e. where there is a high risk that an individual's right to privacy may be infringed such as monitoring or processing special categories of personal data, especially if those initiatives involve large numbers of individuals or new technologies. Such Assessments will allow us to identify and fix problems at an early stage.

8. Data Audits

Personal data will be reviewed and documented annually through a Data Audit. This audit will map the flow of personal data into and out of the Trust.
The annual audit will check the accuracy of the information held. It will ensure that information is not retained for longer than is necessary, and that when obsolete information is destroyed that it is done so appropriately and securely.

Understanding data and how it is being processed is a key step to ensuring compliance with data protection principles.

9. Data Protection Policy Review

Data Protection Policies will be reviewed on an annual basis and published on our websites. Policies intended to be read by children will be explained in clear non–technical language and in a way that can be readily understood.

10. Data Protection Officer

The role of the DPO involves; advising colleagues and monitoring the school's compliance including via staff training and awareness raising; advising on Privacy Impact Assessments; being the point of contact for supervisory authorities; developing policies and procedures; watching out for publication of relevant guidance and Codes of Practice; monitoring the documentation, notification and communication of data breaches.

In line with the requirements of GDPR DPO's will be an expert in their field and have specific knowledge of their sector, which is maintained through training. DPO's must be able to work "independently of instruction". They will report to the highest level of management within the Trust.

To contact the DPO – Email to itroom@farneyclose.co.uk

11. Privacy Notices

Farney Close publishes privacy notices on its website which provide information about processing of personal data for staff, pupils and parents. Privacy Notices must be concise, transparent, intelligible and easily accessible. They must provide information about:

- The school
- Contact details of the DPO
- What personal data is gathered
- The Purpose of processing data and the legal basis for the processing of that data
- Who the personal data is shared with
- Transfers outside EU and how data is protected
- Retention period or criteria used to set this
- Legal rights e.g. the right to withdraw their consent to their data being used

- Right to complain

Privacy notices must be reviewed at regular intervals. Academies must issue an annual privacy notice to all parents, pupils over 18, and employees, before, or as soon as possible after, any personal data relating to them is obtained, and annually thereafter.

12. Legal Grounds

GDPR sets out conditions that must be met for the processing of personal data to be lawful. At least one of these must apply whenever personal data is processed:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The legal grounds for processing personal data is explained in relevant Privacy Notices.

13. Consent

Farney Close will seek consent to process some types of personal data that do not fall under other legal categories outlined above.

'Consent' is defined as any freely given, specific, informed indication of the data subject's wishes by which he or she, by a statement, signifies agreement to personal data relating to him or her being processed. Consent must be unambiguous and be a positive indication of agreement. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent must be freely given and capable of being withdrawn at any time. It must be as easy for an individual to withdraw their consent as it was to provide it in the first place. Clear explanation must be given to individuals what they are consenting to and of their right to withdraw consent.

Separate consents must be obtained for specific processing operations. It must be distinguishable from other matters and not "buried" in wider written agreements.

14. Retention and Security of Personal Data

Farney Close will ensure that personal data is stored, transferred and disposed of securely and in accordance with the retention and disposal schedule. We will ensure that appropriate security measures are in place and enforced to keep paper and electronic personal data secure, making certain that only authorised individuals have access to personal data.

15. Cloud based technologies are utilised; following completion of a data privacy impact assessment prior to implementation, appropriate security measures are in place to secure this data including files being saved in an encrypted form requiring username and password to log into the service to decrypt the files for access. Data is retained in accordance with our data retention schedule which is available on our website. Requests for Access to Personal Data

This section sets out the process that will be followed by Farney Close when responding to requests for access to personal data made by the children or their parent, or an employee.

There are two distinct rights of access to information held by schools about children, parents and staff:

- Under the GDPR 2018 any individual has the right to make a request to access the personal information held about them.
- The right of those entitled to have access to curricular and educational records as defined within the Education (Pupil Information) (England) Regulations 2005.

15.1 Subject Access Requests (SAR)

GDPR gives individuals the right to access personal data relating to them processed by a data controller. Requests may be received by employees, current or past, or by pupils or their parents.

A SAR must be made in writing; which can include email and be addressed to the Data Protection Officer for Farney Close School, which is contracted to the DPO. A SAR request form is available on the staff shared area which covers all the areas required to make a SAR and should be sent out to anyone making a request. Any requests received at the school should be logged with the DPO for processing by the Data Protection Lead. Where the original request does not clearly identify the information required, then further enquiries should be made. Where a request received does not mention the GDPR or SAR, where this meets the criteria this will still be processed as such.

The identity of the requestor will be established before the disclosure of any information is made. All SAR received will be responded to within one month (irrespective of school holiday periods). The month will not commence until after receipt of proof of identity and any necessary clarification of information is sought. There are some exemptions available under the GDPR, which mean that occasionally personal data will need to be redacted (blacked out/removed) or withheld from the disclosure. All information will be reviewed prior to disclosures to ensure that the intended disclosure complies with Farney Close Schools' legal obligations.

Where the personal data also relates to another individual who can be identified from the information the information will be redacted to remove the information that identifies the third party. If it is not possible to separate the information relating to the third party from the information relating to the subject of the request, consideration will be given to withholding the information from disclosure. These considerations can be complex and additional advice will be sought where necessary.

Any information which might cause serious harm to the physical or mental health or emotional condition of the child or another person will be withheld along with

any information that would reveal that the child is at risk of abuse, or information relating to Court Proceedings.

15.1.1 Requests from Pupils

Young People can exercise their rights under the GDPR once they are sufficiently mature. The right can be exercised by a person with parental responsibility on behalf of their child if the child is not able to understand the process or has not reached sufficient maturity.

For the purposes of a SAR, Farney Close will apply the full legal definition of 'parental responsibility' when determining who can access a child's personal data. Proof of the relationship with the child must also be established as this will verify whether the individual making the request can lawfully exercise that right on behalf of the child.

The ability of young people to understand and exercise their rights is likely to develop or become more sophisticated as they get older. It is widely accepted that children of primary school age do not have the maturity to understand or exercise their own rights; and in accordance with guidance from the Information Commissioners Officer (https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/) indicate as a general guide, a child of 12 or older is expected to be mature enough to understand the request they are making.

A child may, of course, be mature enough at an earlier age or may lack sufficient maturity until a later age, and so requests received by Farney Close for data relating to a child/young person will be considered on a case by case basis considering the circumstances surrounding the case and the child.

Where a SAR is received by a person with parental responsibility on behalf of a child over the age of 12 and Farney Close considers the child is mature enough to understand their rights, Farney Close will seek permission from the child for information to be given to the parent before it's disclosed. Farney Close, will, where appropriate, discuss the request with this child in question to ensure they understand rather than relying on a signature. A child with competency can refuse to consent to a request for their personal information made under the Data Protection Act. This position differs when the request is for access to the Education Record of their child (see below for more detail).

15.2 Request for Access to a curricular and education record as defined within the Education (Pupil Information) (England) Regulations 2005.

A parent may make a request to access information contained within their child's education record, regardless of whether the child agrees to the disclosure of information to them. The right of access belongs to the parent in these cases. It is not a right being exercised by the parent on behalf of the child.

For the purpose of responding to an Educational Records request, Farney Close will apply the definition of 'parent' contained within the Education Act 1996. An "*educational record*" means[1] any record of information which-

(a) Is processed by or on behalf of the governing body of, or a teacher at, any school maintained by a local education authority and any special school which is not so maintained.

(b) Relates to any person who is or has been a pupil at any such school; and
(c) Originated from or was supplied by or on behalf of the persons specified in paragraph (3)

Other than information which is processed by a teacher solely for the teacher's own use; The amount that can be charged for a copy of information contained in an education record will depend upon the number of pages provided. The charge made will be in accordance with the Schedule to the Data Protection (subject access) (Fees and Miscellaneous Provisions) Regulations 2000.

No charge will be made to view the education record.

The response time for requests made under the Education (Pupil Information) (England) Regulations 2005 is 15 school days (this does not include half terms or teacher training days).

An exemption from the obligation to comply with the request will be claimed where the disclosure of the information to the parent may cause serious harm to the physical or mental or emotional condition of the child or another person or if the disclosure of the information would reveal that the child is at risk of abuse.

16. Requests for Rectification

GDPR includes the right for individuals to have inaccurate personal data rectified or completed if incomplete. Requests should be made in writing to the Trust Business Manager who will liaise with the DPO and respond within 30 days of receipt. Where any requests are received verbally, they will be asked to complete these in writing. Upon receipt of the request the Trust Business Manager will liaise with the DPO to investigate whether the data held in question is accurate. During this time, access to data, which is being contested will be restricted, wherever possible. A note will be placed on the system/file that the information is being reviewed for accuracy. If data is found to be accurate, the individual will be informed that this will not be amended and will be notified of their right of complaint to the ICO. The file note will be updated to include that the data has been reviewed for accuracy. There may be some exemptions to the right to request rectification such as where these are manifestly unfounded; or excessive. Each request will be considered on a case-by-case basis and in line with guidance from the ICO. Requests for rectification will be added to the MAT Record of Requests Log.

17. Requests for Erasure

Individuals have the right to request that personal data is erased; sometimes termed 'the right to be forgotten.' Requests should be made in writing to the Principal who will liaise with the DPO and respond within 30 days of receipt. Where any requests are received verbally, they will be asked to complete these in writing. Upon receipt of the request the Principal will liaise with DPO to investigate whether the request meets the criteria to be considered for erasure; i.e. if the holding of data is no longer necessary; where the legal reason for holding such data is explicit consent and the consent is withdrawn, where the data is held for purposes of direct marketing or where the data is being processed unlawfully. Where the data is erased from Farney Closes' systems/records; reasonable attempts will also be made to inform other organisations who may hold this data, as disclosed by Farney Close. There may be some further exemptions to the right to request rectification such as where these are manifestly unfounded; or excessive. Each

request will be considered on a case by case basis and in line with guidance from the ICO. Requests for erasure will be added to the FCS Record of Requests Log.

18. Transfers to Third Parties

Requests for data received from third parties, which are not a legal requirement, such as mortgage companies asking for salary information will be logged as a request on the FCS Record of Information Request Log by HR and an overview of responses made. Prior to any information being provided, Farney Close will seek to verify that consent has been provided by the individual.

19. Third Party Suppliers

Farney Close will ensure that any third parties which process data on its behalf ('data processors') meet the requirements set out in article 28 of the GDPR. Supplier contracts where the trust passes data to them, and they receive and store it, such as insurers, payroll and curriculum enrichment providers, are data processors. The Principal is responsible for ensuring that these are GDPR compliant.

The Principal will ensure that all such existing or new third-party suppliers are compliant with data clauses as detailed in paragraph 3 of article 28. A check list taken from this section of the GDPR is included in Appendix 1.

20. Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Personal data breaches can include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.

Farney Close will adopt internal procedures for detecting, reporting and investigating a personal data breach.

Where Farney Close detects a breach, which is subject to the mandatory reporting rules then it will log the breach via GDPRiS seeking guidance regarding whether the breach is reportable. If deemed reportable this will be actioned by the DPO to the supervisory authority without "undue delay" and not later than 72 hours after becoming aware of it. Breaches which are likely to result in an individual suffering damage will need to be reported e.g., breaches that could result in identity theft or where an individual's confidentiality has been breached.

All Breaches are logged electronically Farney Close and advice sought and followed.

Where a breach has to be reported to affected individuals, this will have to be done without "undue delay".

21. Staff Data Protection Training

Farney Close will take organisational steps to keep personal data secure, and the deployment of staff data protection training is key to reducing the likelihood of data losses. Academies will ensure that new starters will receive data protection training, proportionate to their role, before they have access to personal data and existing staff will receive regular and refresher training.

22. CCTV

Images and audio recordings of identifiable individuals captured by Closed Circuit Television amount to personal data relating to that individual and will be subject to the same provisions and safeguards afforded by the GDPR as other types of recorded information.

Farney Close will use CCTV for the following purposes:

- To protect Farney Close buildings and assets
- To support the safeguarding and well-being of staff, children and visitors
- To reduce the fear of crime
- To support the Police in order to deter and detect and to apprehend and prosecute offenders
- To help protect members of the public and private property.

Farney Close will ensure that any use of CCTV is necessary and proportionate and will ensure that regular reviews of the use of CCTV take place.

Farney Close will ensure that any use of CCTV is included in its notification to the ICO.

Farney Close's use of CCTV will comply with the Information Commissioner's Office CCTV Code of Practice https://ico.org.uk/for-organisations/guide-to-dataprotection/cctv/

Farney Close will ensure that clear notices are in place identifying when an individual is entering an area that is monitored by CCTV. The notice will identify Farney Close as the responsible data controller and will state the purpose for which the recording is taking place.

Farney Close will not operate audio recording as part of the CCTV without seeking additional advice. Farney Close will not operate CCTV in any areas of the premises where individuals would have a legitimate expectation of personal privacy, such as toilets or changing rooms.

Farney Close will ensure that CCTV recordings are kept securely and that access to them is restricted to those staff who operate the system or make decisions relating to how the images should be used.

Please refer to local CCTV Policy's published on the Farney Close website.

23. Photographs and Electronic Images

Further information in relation to the use of photographs/videos that contain images of children can be found in Farney Close's Acceptable Use of ICT Policy which all employees sign up to and within Safeguarding Policies. The school has a policy that provides the position regarding parents photographing and filming children at Farney Close events and the use of images of children by the school in any publicity material, its website, in newspapers and in outside agency publications.

24. Biometric Data

If Farney Close uses or intends to use biometric data (such as fingerprint technology) a separate, detailed notice will be sent to all children and parents explaining the intended use and providing parents with options for alternative systems if they wish their child to opt out. The school will obtain the written consent of at least one parent before taking and using and biometric data from a child.

25. Breaches of this Policy

All breaches of confidentiality and information security, actual or suspected, will be reported and investigated under Farney Closes' Disciplinary Policy and Procedure. In accordance with the Disciplinary Policy, serious breaches of the Data Protection Policy will normally be regarded as gross misconduct.

An employee's conduct and/or actions may also be unlawful or illegal and they may be personally liable. Farney Close reserves the right to report any illegal violations to the appropriate authorities.

26. Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong. You can make a complaint at any time by contacting our data protection officer (see section 10 for contact details).

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

27. Who is the schools Data Protection Officer?

As of the 8th June 2021 the schools Designated Data Protection Officer is Ray Lau (Vice Principal). rlau@farneyclose.co.uk

Appendix 1

Supplier contracts - GDPR checklist

Under the General Data Protection Regulation (GDPR) you must ensure that any third parties that process data on your behalf meet the GDPR requirements

- To do this, check the data protection clauses in all contracts that were live when the GDPR came into force (25 May 2018), and any that you've entered into since then
- You must include certain information in contracts with third parties/suppliers (such as insurers, payroll and school club providers) where the school passes data to them, and they receive and store it
- You can add this information as a schedule to the contract, rather than having to amend the whole document
- Our checklist sets out the information that the schedule needs to cover to help you get GDPR-compliant. Use it when amending contracts to make sure you're covering every base. You can also use this when agreeing new contracts
- The information in the checklist is taken from paragraph 3 of article 28 of the GDPR
- Speak to your legal advisers for further support and advice on the process of updating contracts

Supplier contracts – GDPR checklist

INFORMATION TO INCLUDE TO MEET GDPR REQUIREMENTS	COMPLETE?
The subject matter, duration, nature and purpose of the data processing *this information will need to be specific to each contract*	☐
The type(s) of personal data being processed *this information will need to be specific to each contract*	☐
The categories of the data subjects (the individuals whose data is being processed) *this information will need to be specific to each contract*	☐
The obligations and rights of the data controller (your school) *this information will need to be specific to each contract*	☐
The data processer (the third party/supplier) processes data only on the documented instructions of the school	☐
The people who process the data are committed to confidentiality, or are required by law to uphold confidentiality	☐
The third party takes measures to ensure data is processed securely	☐
The third party will not engage another processor without prior written authorisation from the school	☐
If the third party does engage another processor, this processor will be bound by a written contract with the same data protection conditions as are in the contract with the school	☐
The third party helps the school comply with: • Upholding the data rights of individuals • Secure processing • Reporting and communicating data breaches • Conducting impact assessments where relevant	☐
The third party deletes or returns the personal data to the school at the end of the provision of services (unless the law states that the information must be kept)	☐
The third party makes information available to the school to demonstrate its compliance with the obligations in the contract, and allows the school or another party instructed by the school to conduct audits and inspections	☐