FARLEIGH

2.08 DATA PROTECTION POLICY

This policy applies to:	~~Pupils /~~ Staff ~~/ Visitors / All~~ Prep / Pre-Prep / Kindergarten Day / Boarding
Person(s) responsible:	Director of Finance and Operations
Last updated:	December 2025 *(light review in Jan 26 to reference DUAA)*
Review period:	12 months
Next review:	December 2026
This policy should be read in conjunction with:	2.09 Privacy Notice for Parents and Pupils 2.10 Privacy Notice for Staff, Volunteers, Governors and Job Applicants 2.11 Retention of Records

1. Background

Data protection is an important legal compliance issue for Farleigh School. During the course of the school's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the school's Privacy Notices). The School, as "data controller", is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the school's culture and all its staff and representatives need to be mindful of it.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR), the Data Protection Act 2018 (DPA 2018) and the UK Data (Use and Access) Act 2025 (DUAA 2025). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

2. Definitions

Key data protection terms used in this data protection policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the school is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information (or 'personal data'):** any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the school's, or any person's, intentions towards that individual.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- **Special categories of personal data –** data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

3. Application of this policy

This policy sets out the school's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or governors of the school are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the school or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the school's personal data as contractors, whether they are acting as "data processors" on the school's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the school shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

4. Person responsible for Data Protection at the school

The School has appointed the Director of Finance and Operations (DFO) (bursar@farleighschool.com) as the Information Management Officer who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Information Management Officer.

5. The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's broader 'accountability' principle also requires that the school not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notices were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

6. Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the school to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the school. It can be challenged by data subjects and also means the school is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notices, as GDPR requires. Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7. Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the school is accurate, fair and adequate. Staff are required to inform the school if they believe that *any* personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the school's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with this Policy and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the school's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Child Protection and Safeguarding
- Low Level Concerns
- Use of Electronic Devices, Mobile Phones and Cameras
- Staff and Visitors Acceptable Use of ICT
- E-Safety
- Social Media

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Data Protection Impact Assessments

A data protection impact assessment (DPIA) will be conducted whenever a new service involving personal data is being developed. The DPIA will be divided into two elements: (1) screening and (2) full DPIA. It is the responsibility of all activity owners to complete a screening questionnaire (as outlined at *Annex A*) which will be used by the DFO to determine if a full DPIA is required.

Third Parties and Data Transfers

Any third-party business service providers working with or for the school that have, or might have, access to personal data will be expected to have read, understood and to comply with this policy. All third-party processors must commit to complying with GDPR, and must have a contract in place (with suitable data protection clauses) before the processing of data commences. Any sub-processors appointed by the third-party must be approved, in writing, by the school.

All exports of data from within the European Economic Area (EEA) to third countries, outside the EEA, must have an adequate level of protection in place. Whenever a third-party processor intends to, or is, processing data in a third country, the Information Management Officer must be informed without delay.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify the DFO. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the school always needs to know about them to make a decision.

As stated above, the school may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the school, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

The procedure for managing a Data Breach is outlined at *Annex B*.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the school to the DFO and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

Retention and Disposal of Data

Personal data may only be deleted or disposed of in line with the archiving procedures of the school, laid down in the Retention of Records Policy (2.11).

8. Rights of Individuals

In addition to the school's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the school). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the DFO as soon as possible.

The Data Subject Access Request (DSAR) procedure is laid down at *Annex C*.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply.

However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);

- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the DFO as soon as possible.

9. Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Where a worker is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted.
- Use of personal email accounts or unencrypted personal devices by governors or staff for official School business is not permitted.

10. Processing of Financial / Credit Card Data

The School complies with the requirements of the Payment Card Industry Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the school Accountant. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

11. Appropriate Policy Document

The DPA 2018 requires there to be an Appropriate Policy Document to be in place when processing criminal convictions/offences data and special category data that meet the specified conditions in Parts 1, 2 or 3 of Schedule 1 of the DPA 2018. This is laid down in *Annex D* to this Policy.

Annex A Data Protection Impact Assessment (DPIA) Screening Questionnaire.

Annex B Data Breach Procedure.

Annex C Data Subject Access Request (DSAR) Procedure.

Annex D Appropriate Policy Document.

Annex A – Data Protection Impact Assessment (DPIA) Screening Questionnaire

SCOPE

All new processing activities that involve processing personal data of employees, customers or consumers that require a data protection impact assessment (DPIA) are within the scope of this procedure.

RESPONSIBILITIES

Activity Owners are responsible for completing a DPIA screening questionnaire for each new processing activity that is undertaken. Each completed DPIA will be submitted to the DFO for approval. Activity Owners are responsible for ensuring that the actions agreed in the DPIA are fully implemented and transitioned into operations.

CONDUCTING A DATA PROTECTION IMPACT ASSESSMENT

There are two elements to conducting a DPIA; (1) the completion of a screening questionnaire, and (2) the completion of a full DPIA. The objective of the screening questionnaire is to understand whether an activity involves the processing of personal data and whether it needs a full DPIA completed.

A full DPIA will only be required if the activity that is being undertaken is likely to result in a high risk to data subjects or new technology. If the activity is part of a repeatable process a DPIA will not need to be conducted.

PROCEDURE FOR COMPLETING A DPIA

4.1 DPIA Screening Questionnaire

Each new activity that is undertaken in the school will complete a DPIA Screening Questionnaire. This will ascertain the need for conducting a full DPIA. The relevant Activity Owner will review the output, engage the DFO as required and sign off the document when an agreed way ahead has been obtained.

Where there are positive (yes) responses to the screening questions, the Activity Owner must contact the DFO to confirm whether or not a full DPIA is required.

A copy of the completed DPIA screening questionnaire should be filed, enabling access for review and audit purposes.

4.2 Full Data Protection Impact Assessment (DPIA)

Where a full DPIA needs to be conducted the DPIA template should be downloaded and completed. This comprises of 6 sections:

Personal Data Collection

This section looks at the personal data that is collected, transmitted, stored, accessed or deleted as part of the activity. Each piece of personal data that is being used should be incorporated into this section of the form.

Data Processing

The objective of this section is to understand why the data is being processed, the school's role, who is responsible for it and how it will be managed.

Data Ownership

This section aims to understand which parts of the school will process the personal data and identify ownership of the data within the school.

Privacy Risks

This section looks to identify the potential risks to the individual (data subject) of the intended processing. All of these should be thought through and captured.

Risk Mitigation

This section aims to identify the actions that will be required to remediate the privacy risks that have been identified.

Summary

This is the consolidation of the above information.

When completed the DPIA should be signed off by the Acticity Owner before being sent to the DFO. The DFOwill review the document, raise any issues and once it has been confirmed that the privacy risks have been identified and suitable action plan put in place, and will approve and sign off the document.

Where there are any disputes over the risks or required actions, these will be escalated to the DFO.

4.3 Implementation

It will be the responsibility of the Activity Owner to ensure that each of the actions identified in the DPIA to mitigate the privacy risks are implemented as part of the project. Any failure should be notified to the Privacy Officer without undue delay.

GLOSSARY

Term	Definition
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processor	A data processor is responsible for processing personal data on behalf of a data controller.
Information Management Officer (DFO)	The Information Management Officer is an enterprise leadership role reporting to the risk committee. The privacy officer is responsible for overseeing the school data protection strategy and implementation to ensure compliance with GDPR requirements. At Farleigh School this is the DFO.
Data Subject	Any living individual who is the subject of personal data held by an organisation.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Privacy Notice	An outward facing document that provides transparent and accessible information to individuals about how Farleigh School uses their personal data. This can be found on the website.

DPIA SCREENING QUESTIONNAIRE

Instructions

1. This form should be completed for each processing that is initiated across Farleigh School ("the school").
2. The completed form should be stored and be available for review and audit purposes.
3. The questions below should be answered 'Y' = Yes or 'N' = No, and a brief description of the intended processing / activity completed.
4. If the answer to Q1 is No, no further responses are required and a DPIA will not need to be conducted.
5. Once completed, the person completing the form should enter their details and date of completion.
6. The form should be submitted to the activity owner to sign off the information provided.

	Screening questions	Y/N	Description of Activity
Q1	Will the processing activity involve the handling of personal data pertaining to employees, pupils, parents, visitors, governors, contractors or volunteers?" If "No" please exit the questionnaire.		
Q2	Is the personal data being used already collected by the school? If, so are you using the data for a purpose other than it was originally collected for?		
Q3	Is the data being processed of a sensitive nature? If so, please describe.		
Q4	Will the processing result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		
Q5	Will information about individuals be disclosed to third parties or people who have not previously had routine access to the information?		
Q6	Where personal data is shared with a third party will it be part of a process outsource, cloud or hosted service? Please state.		
Q7	Will the personal data be held in a country outside of the European Economic Area (EEA)? Which country (if known)		
Q8	Does the processing involve you using new technology or areas listed in the description of activity column opposite.		Process Special Category Data, Process Biometric or Genetic Data, Process data involving people's online or offline location or behaviour, Process Children's data.

If you have answered '**Yes'** to any of the above questions you should share this document with your local Data Owner or Data Champion who will advise whether a full data protection impact assessment needs to be completed.

Completed By: Role: Date:

Approved By: Role: Date:

Annex B – Data Breach Procedure

SCOPE

This procedure applies to the activities that employees, contractors or temporary staff in Farleigh School ("the school") should undertake in the event of becoming aware of any personal data, security incident or breach occurring in order to meet the requirements of Data Protection Legislation in the handling of a personal data breach (henceforth "personal data breach" or "data breach").

DEFINITIONS

A "security incident" is an unplanned interruption to an IT service that may be caused by a breach of the Information Security Policy or a failure in the security measures.

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

Personal data breaches will be categorised according to the following principles

1) **Confidentiality** – an unauthorised or accidental disclosure of, or access to, personal data.
2) **Integrity** – an unauthorised or accidental alteration of personal data
3) **Availability** – unauthorised or accidental loss of access to, or destruction of, personal data.

A personal data breach will always be a security incident, but not all security incidents will be a personal data breach. Examples of Data Breaches include:

- a lost or stolen laptop, USB flash drive or mobile phone;
- an email sent to the wrong recipient;
- an unauthorised person gaining access to a laptop, email account or computer network, e.g. through hacking, a malware attack or a phishing email;
- unauthorised access to a data storage system (such as an HR or CRM system); and
- an accidental update of a database that leads to incorrect data being written to individuals' records.

RESPONSIBILITY

The Governors of the school have responsibility for ensuring that any privacy risks are managed.

All users of information assets across the organisation should familiarise themselves with this procedure, be aware of privacy risks and be vigilant to ensure breaches are identified, reported and managed in a timely manner.

All staff are responsible for reporting mistakes, suspected or actual data breaches at any given time. They must report all incidents, including those resulting from human error and those with unidentified or unknown affected data subjects as soon as detected.

Support will be provided to ensure everyone has access to the appropriate skills and training to carry out their role effectively. However gross negligence and intentional violations (including not reporting incidents/mistakes) are taken seriously and could lead to disciplinary action.

INITIAL ASSESSMENT OF A BREACH

When any employee, contractor or temporary worker becomes aware of or is informed of an IT incident or personal data breach, they should immediately report the matter to the school's Information Management Officer (the DFO – on extension 2803, or by email to bursar@farleighschool.com) or, in his absence, the Headmaster or other member of the Senior Management Team.

The School will make an initial assessment of the breach, considering the following questions:

- How long has the breach been active?
- What data was involved?
- How far has it got/how widely dispersed is the information?

The School will then seek to contain and recover the information as far as possible, considering the following factors (among others):

- if a cyber breach, involve the school's IT personnel from the outset;
- if human factor(s) are involved, can they be contacted to give reassurances;
- if e.g. Royal Mail, courier, IT or other contractors are involved, can they assist;
- are specialists needed: forensic IT consultants, crisis management PR, legal etc.

MANAGING A DATA BREACH

The School aims to complete a preliminary investigation of all reported incidents without undue delay, with an aim to establish its awareness of a personal data breach within the first 24 hours of internal detection.

From that point, there are 72 hours within which to identify whether there is a significant risk to the concerned data subjects and where there is a risk, notification to the supervisory authority should take place. In these first 72 hours of any data breach being identified, the school will seek to build up a more detailed picture of the risk and reach of the security breach, considering:

- how many have been affected?
- was any sensitive personal data involved – for example health in medical notes, or crime in employment records?
- was financial data involved and/or is there a risk of identify fraud?

The school will consider whether a crime has been committed and therefore whether to involve police or the cyber crime unit. The school would have no hesitation in reporting any matter that they suspected of being a crime. The school would consider if insurers need notifying, as the breach may amount to a major loss, crime, or possible legal claim.

The School, as part of its assessment, will consider whether the breach would lead to the likely risk of harm to the data subjects and therefore if it:

- is sufficient to require a full or preliminary notification to the Information Commissioner's Office (ICO – see section 7); and
- is sufficiently serious to require communication to affected individuals.

When considering reporting to agencies or to individuals the school will assess:

- if not considered to have met the reporting threshold, is this a matter we can document but deal with internally?; or
- if it has met the threshold, what can we usefully tell the ICO and/or individuals at this stage?
- If the school should provide fraud or password advice, offer counselling etc.

BREACH REPORT FORM

The Information Management Officer will contact the relevant Data Owner(s) to confirm the scope and impact of the breach without delay and ask them to log the breach in the Data Breach Log.

The record will require the following information to be provided:

- Name and contact details of the individual who reported the incident
- Impacted area and date of the breach

- Description of the incident
- Details of personal data that are involved
- Any impacted individuals or groups of individuals, if known

An assessment of the level of risk posed to data subjects as a result of the incident will be undertaken and documented. Where there is a high risk to data subjects the ICO will be informed, see below.

REPORTING PERSONAL DATA BREACHES

Information Commissioner's Office (ICO)

All personal data breaches which pose a risk to the rights and freedoms of data subjects must be reported to the Information Commission's Office (ICO) within 72 hours of becoming aware of a relevant breach. If the data breach notification to the ICO is not made within 72 hours, the Information Management Officer will submit the notification electronically with a justification for the delay.

The following information needs to be provided to the ICO by the Information Management Officer:

- A description of the nature of the breach.
- The categories of personal data affected.
- Approximate number of data subjects affected.
- Approximate number of personal data records affected.
- Name and contact details of the DPO.
- Consequences of the breach.
- Any measures taken to address the breach.
- Any information relating to the data breach.

In the event the supervisory authority assigns a specific contact in relation to a breach, these details are to be recorded in the incident register.

Serious breaches will be reported by the Information Management Officer (or another member of the Senior Management Team in his absence) to:

The ICO

- the security breach helpline 0303 123 1113 (open Monday to Friday, 9am to 5pm); selecting Option 3 to speak to staff who will record the breach and give advice; or,
- the security breach notification form, which should be sent to the email address: icocasework@ico.org.uk; or,
- by post to the ICO at: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The security breach notification form is here: https://ico.org.uk/for-organisations/report-a-breach/.

Any Impacted Data Subject

Where there is a high risk to the rights and freedoms of the impacted data subject(s), the Information Management Officer will notify the data subjects affected immediately.

The notification to the data subject will describe the incident in clear and plain language, in addition to providing the following information:

- A description of the nature of the breach.
- The categories of personal data affected.
- Approximate number of data subjects affected.
- Approximate number of personal data records affected.
- Name and contact details of the DPO.

- Likely consequences of the breach.
- Any measures taken to address the breach.
- Any information relating to the data breach.

If the breach affects a high volume of data subjects and personal data records, the Information Management Officer will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder their ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.

If the Information Management Officer has not notified the data subject(s) and the ICO that it considers the likelihood of a data breach will result in high risk, they will communicate the data breach to the data subject.

QUESTIONS?

If you have any questions about this Policy, please contact the DFO (bursar@farleighschool.com).

Annex C – Data Subject Access Request (DSAR) Procedure

INTRODUCTION

The UK General Data Protection Regulation (UK GDPR) grants all individuals the right to access their personal data held with any establishment and to exercise that right easily and at reasonable intervals, to be aware of, and verify, the lawfulness of the processing.

This procedure defines the internal handling of Data Subject Access Requests (DSAR) received by Farleigh School ("the school"). This Procedure describes how the school must address complaints or requests from Individuals, such as employees, applicants, pupils, suppliers or (website) visitors, regarding the processing of their Personal Data to ensure such requests are dealt with in a structured, transparent and fair manner.

DEFINITIONS

"**Information asset"**	refers to a set of data in hardcopy/ manual or electronic format (e.g. paper records, databases, systems)
"**Data subject"**	means the person which the personal data relates to
"Personal data"	this is data which relates to a living individual who can be identified (a) from that data, or (b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
"Redaction"	means permanently and securely removing data that is exempt from disclosure from the material released to the requestor.
"**Sensitive personal data"**	refers to trade union membership, sexuality, race or ethnicity, religious beliefs, political opinions, health and criminal records.
"**Employment records"**	this is information held by the controller which relates to a member of staff, present, past or prospective, whether permanent, temporary or a volunteer.
"Data Protection Legislation"	Data Protection Legislation means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

SCOPE

All personal data processed by the School is within the scope of this procedure. Example are:

- Name(s);
- Email/postal address;
- Telephone number;
- Account data and electronic identification data (including data added thereto) such as IP address, MAC address, and the data added to specific accounts, such as password, date of birth, gender, language of preference and other information shared;
- Photograph;
- Ethnicity;
- Physical or mental health information;
- Financial account information, such as bank account details;
- Salary;

- Performance evaluations;
- Religious or philosophical beliefs;
- Sexual orientation; and
- National identification number (BSN).

Data subjects are entitled to obtain:

- Confirmation as to whether the School is processing any personal data about that individual.
- Access to their personal data.
- Any related information.

RESPONSIBILITIES

The Information Management Officer (the DFO) is responsible for the application and effective working of this procedure. Once received, the Information Management Officer will investigate and respond to the request accordingly, taking into account the requirements of the Data Protection Legislation in force at the time. They are also responsible for ensuring the school's DSAR Log is maintained and up to date.

Responsibilities of all other employees

All other employees are prohibited from responding to any data subject access request and for the purposes of this policy are defined as "unauthorised employees".

- In the event that a data subject access request is received by an unauthorised employee, details of the request and any accompanying documents are to be forwarded to bursar@farleighschool.com.
- Data Owners are responsible for informing the Information Management Officer whenever a DSAR is received, without delay.
- Where a DSAR is received from an external source, vial letter or mail, it should be passed to the Information Management Officer without delay.
- In the event that any communication is received from the Information Commissioner's Office (ICO – the UK Supervisory Authority), the Information Management Officer is to be informed immediately.

PROCEDURES FOR HANDLING SUBJECT ACCESS REQUESTS

5.1 Subject Access Request from an Individual

The following people can submit a data subject access request:

- The individual themselves.
- Individuals requesting access on behalf of a child for whom they have parental responsibility.
- A representative nominated by the individual to act their behalf such as solicitors or a relative, where there is valid consent by the individual granting this authority.

DSARs can be made in any form, including via post, email, telephone and social media. It may be helpful, however, to use the Notification of DSAR Form below to help elicit exact what information is being sought.

Individuals can initiate a request verbally and where this is the case, the request should be confirmed with the individual and put in writing by the person to whom the request has been made and emailed to bursar@farleighschool.com.

When a DSAR request is initiated on behalf of an individual by a third party such as a solicitor they must provide evidence of written authority from the individual they are making the request on behalf of. Only once this is received will the request be processed.

Any request received from a non-employee will require the individual to provide **evidence of their identity**. This should be a copy of forms of identification such as Passport, Driving licence, Birth certificate, Utility bill (from last 3 months), Current vehicle registration document, Bank statement (from last 3 months). Where the evidence of identity is not adequate it should be documented and a further request made to the data subject. On receipt of suitable evidence of identity, a confirmation of receipt for the request will be sent to the individual.

The Information Management Officer will identify the Departments that will be required to support the DSAR process. These will be contacted in the first instance to confirm that they hold data on the named individual. After confirmation, they will be requested to provide copies of the personal data they hold in electronic and paper formats.

The Information Management Officer will consolidate the information provided and determine what should form the content of the DSAR, engaging with the Department as required.

5.2 Subject Access Request from an Employee

The employee will initiate the DSAR by sending an email to bursar@farleighschool.com.

Employees can initiate a request verbally and where this is the case, the request should be confirmed with the employee and put in writing by the person to whom the request has been made and emailed to bursar@farleighschool.com.

No identification will be required as long as the employee is known to the school and a notification of receipt of request will be sent to the employee.

INFORMATION TO BE PROVIDED IN A SUBJECT ACCESS REQUEST

6.1 Data Collection

Data collection entails the following;

- Collecting the data specified by the Data Subject.
- Collecting the data relating to the Individual routinely handled as part of daily activities
- Where additional information is requested from the Individual, collection will include reasonable efforts to search all databases and all relevant filing systems, including all back up and archived files (computerised or manual) and all email folders and archives.
- Where third parties are involved in the processing of the Individual data and additional information is held by them, the subject access request should be communicated with them and the data received.

6.2 Contents of the Response

When an Individual requests what personal data is being processed on them under a DSAR then the following information must be provided in the response:

- Purpose of the processing.
- Categories of personal data.
- Recipient(s) of the information, including recipients in third countries or international organisations.
- How long the personal data will be stored.
- The data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed.
- Inform the data subject of their right to lodge a complaint with the School about the way their personal data has been handled or to raise a complaint directly with the supervisory authority, the ICO.
- Information on the source of the personal data if it hasn't been collected from the data subject.
- Inform the data subject of any automated decision-making.
- If and where personal data has been transferred and information on any safeguards in place.

6.3 Exemptions

If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided in a DSAR:

- Crime and taxation
- Regulatory activity
- Publicly available information
- Disclosures required by law
- Legal advice and proceedings
- Confidential references.
- Management Information
- Negotiations
- Personal data processed for, or in connection with, a corporate finance service involving price-sensitive information.

TIMESCALE

The Information Management Officer must comply with a subject access request without undue delay and in any event within one calendar month of the date on which the request is received or (if later) the day on which we received any information requested to confirm the requester's identity.

If more time is needed to respond to complex requests, an extension of another two months is permissible. This should be communicated to the data subject in a timely manner within the first month.

If the Information Management Officer, on behalf of the School, cannot provide the information requested, the data subject should be informed of this decision without delay and at the latest within one month of receipt of the request.

NOTIFICATION OF DSAR FORM

Please complete this form with details of the request received and forward it to the Information Management Officer (DFO) via bursar@farleighschool.com. Please ensure that any supporting or relevant documents are also attached.

Name of the requesting data subject	
Date of the request *(Please provide the date the request was made by the data subject)*	
Date of receipt of the request *(Please provide the date you received or became aware of the request)*	
Contact details provided by the data subject	
Details of the request *(please provide details of what the data subject is requesting)*	
Method by which request was made *(e.g. email, telephone, social media)*	
Preferred method of communication stated by the data subject *(e.g. email, telephone, social media)*	
Any additional information *(Please provide any additional information that may assist in the handling of the request e.g. any special needs of the data subject)*	
Name and department of the receiver of the request	
Should more information be required, please provide contact details via which you may be contacted to further discuss the request	

Annex D – Appropriate Policy Document

1. OVERVIEW

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document to be in place when processing criminal convictions/offences data and special category data that meet the specified conditions in Parts 1, 2 or 3 of Schedule 1 of the DPA 2018.

2. PURPOSE

The purpose of this policy is to explain the Farleigh School ("the school") procedures for securing compliance with the data protection principles set out in Article 5 of the UK General Data Protection Regulations (UK GDPR) and demonstrate that the school's processing of special category data and/or criminal convictions/offences data based on the specified conditions set out in Schedule 1 of the DPA 2018 comply with Data Protection Law.

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data (including all special category data and criminal convictions/offences data we process) as well as our lawful basis for processing in our privacy notice.

3. SCOPE

The policy details the Schedule 1 conditions for processing and the safeguards we have in place when we process special category data, criminal convictions data. The information in this document satisfies the requirements of Schedule 1, Part 4 of the DPA 2018 and supplements our privacy notice and staff privacy notice.

All staff, contractors and other authorised third parties must adhere to this policy.

4. POLICY STATEMENT

4.1 Conditions for processing special category data, criminal convictions/offences data

Conditions for processing

The School processes the following categories of data:

1. Union membership

Purpose: Part of Payroll processing

UK GDPR Provision:

UK GDPR Article 6 (b) Contract

UK GDPR Article 9 (b) Employment, social security and social protection

DPA 2018 Provision: DPA 2018 Schedule 1, Part 1, 1(1)(a)

2. Ethnicity

Purpose: Equality monitoring – Staff: to help measure organisation performance and improvement in relation to equality and diversity.

UK GDPR Provision:

UK GDPR Article 6 (e) Public Task

UK GDPR Article 9 (g) Reasons of substantial public interest (8),

UK GDPR Article 9 (b) Employment, social security and social protection

DPA 2018 Provision: DPA 2018 Schedule 1, Part 1, 1(1)(a), DPA 2018 Schedule 1, Part 2, 8 (1)

Purpose: Equality monitoring – Pupil: to help measure organisation performance and improvement in relation to equality and diversity.

UK GDPR Provision:

UK GDPR Article 6 (e) Consent

UK GDPR Article 9 (g) Reasons of substantial public interest (8)

DPA 2018 Provision: DPA 2018 Schedule 1, Part 2 8 (1) (b)

3. Health

Purpose: Employee welfare

UK GDPR Provision:

UK GDPR Article 6 (b) Contract

UK GDPRA Article 6 (c) Legal Obligation

UK GDPR Article 9 (b) Employment, social security and social protection

DPA 2018 Provision: DPA 2018 Schedule 1, Part 1, 1(1)(a), 2 (1), 2 (2) (a), 2 (2) (b)

Purpose: Pupil welfare

UK GDPR Provision:

UK GDPR Article 6 (e) Public Task

UK GDPR Article 9 (g) Reasons of substantial public interest (13)

DPA 2018 Provision: DPA 2018 Schedule 1, Part 2 16 (1) (a), 16 (2) (c)

4. Sexual orientation – not requested, but where provided by the individual

Purpose: Pupil welfare

UK GDPR Provision:

UK GDPR Article 6 (e) Public Task

UK GDPR Article 9 (g) Reasons of substantial public interest (8)

DPA 2018 Provision: DPA 2018 Schedule 1, Part 2 16 (2) (d)

5. Religious beliefs – not requested, but where provided by the individual

Purpose: Pupil welfare

UK GDPR Provision:

UK GDPR Article 6 (e) Public Task

UK GDPR Article 9 (g) Reasons of substantial public interest (8)

DPA 2018 Provision: DPA 2018 Schedule 1, Part 2, 8 (1) (b)

6. Criminal offences

Purpose: Staff recruitment

UK GDPR Provision:

UK GDPR Article 6 (c) Legal Obligation

UK GDPR Article 6 (d) Vital Interest

UK GDPR Article 6 (e) Public Task

UK GDPR Article 9 (b) Employment, social security and social protection

UK GDPR Article 9 (g) Reasons of substantial public interest (8)

DPA 2018 Provision: DPA 2018 Schedule 1, Part 1, 1 (1) (a)

Purpose: Pupil enrolment

UK GDPR Provision:

UK GDPR Article 6 (d) Vital Interest

UK GDPR Article 6 (e) Public Task

UK GDPR Article 9 (g) Reasons of Substantial Public Interest

UK GDPR Article 10 Criminal convictions and offences

DPA 2018 Provision: DPA 2018 Schedule 1, Part 2, 12 (1)

7. Criminal convictions

Purpose: Staff recruitment

UK GDPR Provision:

UK GDPR Article 6 (c) Legal Obligation

UK GDPR Article 6 (d) Vital Interest

UK GDPR Article 6 (e) Public Task

UK GDPR Article 9 (b) Employment, social security and social protection

UK GDPR Article 9 (g) Reasons of substantial public interest (8)

DPA 2018 Provision: DPA 2018 Schedule 1, Part 1, 1 (1) (a)

4.2 Procedures for ensuring compliance with the principles

As required by Data Protection Law, we ensure that all processing of personal data at the school is carried out in compliance with the data protection principles.

i. Accountability principle

The School takes responsibility for complying with the UK GDPR and DPA 2018, at the highest level of management and throughout our organisation. We keep records of the steps we take to comply and review and update our accountability measures at appropriate intervals. The technical and organisational measures we have in place include:

- maintaining records of our processing activities;
- adopting and implementing data protection policies;
- reviewing data protection, privacy and information security risks regularly;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to the interests of individuals;
- implementing appropriate security measures and taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
- putting written contracts in place with organisations that process personal data on our behalf; and
- appointing a data protection officer.

ii. Principle (a) – lawfulness, fairness and transparency

The School ensures that data is processed in a lawful, fair and transparent manner.

Lawfulness: We do not do anything unlawful with personal data:

- We identify an appropriate lawful basis for all our personal data processing.
- If we process special category data or criminal offence data, we ensure that we identify a condition for processing this type of data.

Fairness: We do not deceive or mislead people when we collect their personal data:

- We consider how the processing may affect the individuals concerned and can justify any adverse impact.
- We only handle personal data in ways individuals would reasonably expect, or we can explain why any unexpected processing is justified.
- We do not deceive or mislead people when we collect their personal data.

Transparency: We are open and honest with the individuals whose data we process:

- We inform individuals through privacy notices about how their personal data will be processed, who it will be shared with and how long it will be retained.
- We update our privacy notices when we change the purpose for processing personal data and inform individuals.

iii. Principle (b) – Purpose Limitation

We ensure that we clearly identify our purposes for processing any personal data.

- We include details of our purposes in our privacy notice to individuals.
- We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.
- If we plan to use personal data for a new purpose where we have no legal obligation, we check whether the new purpose is compatible with our original purpose, we seek specific consent for the new purpose.

iv. Purpose (c) – Data Minimisation

We know what personal data we hold and why we need it:

- We only collect personal data we actually need for our specified purposes.
- We periodically review the data we hold and delete anything we don't need.

v. Purpose (d) – Accuracy

We ensure the accuracy of any personal data we create:

- We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
- We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.
- If we need to keep a record of a mistake, we clearly identify it as a mistake.
- Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.

vi. Purpose (e) – Storage Limitation

We carefully consider and can justify how long we keep personal data:

- We have a retention schedule which indicates the retention periods where possible.
- We regularly review our information and erase or anonymise personal data when we no longer need it.
- We have appropriate processes in place to comply with requests for erasure where appropriate.

vii. Purpose (f) – Integrity and Confidentiality (Security)

We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place:

- We have an information security policy and take steps to make sure the policy is implemented.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the personal data we process.

- We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- We ensure that any data processor we use also implements appropriate technical and organisational measures.

4.3 Retention and deletion policy

All data is stored and deleted in line with our Retention Schedule.

5. RELATED DOCUMENTATION

- Retention Schedule
- Privacy notice
- Employee Privacy notice

6. CONTACTS

If you have questions about this policy, please contact bursar@farleighschool.com.