



Data Protection Policy

Version:	9.0	
Written by:	ELAN executive team	
Reviewed by:	ELAN Board	Date: 21/07/2026
Approved by:	Name: Rosemary Carr Signed by: Rosemary Carr Chair of the Board	Date: 21/07/2026
Adopted by Academies:	Banwell Primary School Bournville Primary School Locking Primary School Mead Vale Primary School Mendip Green Primary School Milton Park Primary School Oldmixon Primary School Walliscote Primary School Windwhistle Primary School	
Review:	Annually	
Next Review Due By:	July 2027	

Document Control

Document Information

	Information
Document Name	Data Protection policy
Document Author	HR Operations Manager
Document Approval	HR Lead/DPO
Document Status	Version 9.0
Publication Date	July 2026
Review Date	July 2027
Distribution	Website/General

Version Control

Version	Issue Date	Amended by	Comments
1.0	01/07/2018		Board approved
2.0	24/09/2019	HR Manager	Updated to reflect current legislation
3.0	22/10/2019	HR Manager	Separated data retention schedule.
4.0	09/12/2020	HR Manager	Annual review – no update
5.0	July 2022	Head of HR/DPO	Annual review updates to clarify definitions or procedures
6.0	Oct 2023	Head of HR/DPO	Annual review, minor amendments and update ELAN address
7.0	July 2024	HR/Data Manager	Annual review – minor amendments
8.0	July 2025	HR/DPO/Data Manager	Annual review
9.0	July 2026	HR Operations Manager	Legal framework – added in additional reference policy, artificial intelligence (AI) Statement of intent – added in employees are required to comply with policy Role & Responsibilities- employees – added in timeframes for responses Data breach – notify DPO within 24 hours. Failure to comply may result in disciplinary action Data security – added in using multifactor identification. Inclusion of complaints section and appendix 1 – data protection complaints process

Contents

1. Statement of intent.....	4
2. Legal framework	5
3. Definitions	5
4. The data controller.....	6
5. Principles	6
6. Roles and responsibilities	7
7. Collecting personal data	8
8. Limitation, minimisation and accuracy	8
9. Sharing personal data.....	8
10. The right of access	9
11. Additional rights in relation to data	11
12. Parental requests to see educational records	11
13. Privacy by design and privacy impact assessments.....	11
14. Data security	12
15. Disposal of records.....	13
16. Data breaches	13
17. Publication of information	15
18. CCTV and photography	15
19. DBS data	16
20. Training	16
21. Complaints	17
22. Policy review	17
Appendix 1 – Data Protection Complaints Process	18

1. Statement of intent

Extend Learning Academies Network (ELAN) and the schools that make up the multi academy trust (MAT) will ensure that all personal data collected about employees, pupils, parents, governors, visitors, contractors, suppliers and other individuals in any way lawfully associated with ELAN or any of its schools, is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Any reference to ELAN within this policy applies to any or all of its schools and central locations as appropriate.

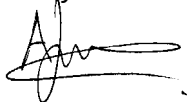
This policy should be read in conjunction with ELAN's privacy notices for pupils, staff, governors and suppliers, contractors and volunteers. All staff are required to comply with this policy at all times. Failure to do so may result in disciplinary action.

ELAN and/or its schools may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the local authority (LA,) and Department for Education (DfE), other schools and educational bodies, and potentially children's services.

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

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

Signed by:

A handwritten signature in black ink, appearing to be 'A. ...'.

CEO

Date:

21/07/2026

A handwritten signature in black ink, appearing to be 'R. ...'.

Chair of Board

Date:

21/07/2026

2. Legal framework

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018.

It is based on published guidance on the UK GDPR by the Information Commissioner's Office (ICO) and the ICO's code of practice for data subject access requests (DSARs).

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

This policy also complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. This policy will be implemented in conjunction with the following other ELAN policies:

- ICT and Online Safety Policy
- Freedom of Information Policy
- Data Retention Policy
- Use of Artificial Intelligence (AI)

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: ○ name (including initials) ○ identification number ○ location data ○ online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ○ racial or ethnic origin ○ political opinions ○ religious or philosophical beliefs ○ trade union membership ○ genetics ○ health – physical or mental ○ sex life or sexual orientation ○ biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable living individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	a person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The Extend Learning Academies Network (ELAN) is the data controller for the use of personal data relating to pupils, employees, governors, contractors, visitors and others e.g. parents.

ELAN is registered with the ICO and will renew this registration annually or as otherwise legally required to do so.

5. Principles

The GDPR is based on data protection principles that our Schools must comply with. The principles are that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the schools aim to comply with these principles.

6. Roles and responsibilities

This policy applies to all employees of ELAN and to other external organisations or individuals working on our behalf, whether in ELAN schools or central location.

ELAN trustees

The trustees have overall responsibility for ensuring that ELAN schools and central location comply with all relevant data protection obligations.

Employees

Employees are responsible for:

- collecting, storing and processing any personal data in accordance with this policy and all relevant Privacy Notices
- informing ELAN of any changes to their personal data, such as a change of address
- contacting the Data Protection Officer (DPO) in the following circumstances:
 - if they have any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - if they have any concerns that this policy is not being followed
 - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK if there has been a data breach, employees must report all actual or suspected data breaches within 24 hours
 - if they engage in a new activity that may affect the privacy rights of individuals whenever that happens
 - if they need help with any contracts or sharing personal data with third parties.
 - If they have received a Data Subject Access Request (DSAR) ELAN has one calendar month to respond. Once the information has been compiled and third party redaction completed by the school, the DPO needs to review this before it is shared with the requesting party.
 - If they have received a Freedom of Information request (FOI), ELAN have 20 working days to respond.

Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will report their activities to the trustees and, where relevant, report to the trustees their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

The DPO within ELAN is Michelle Clarke (Head of HR), who is contactable via:
Email at HR@extendlearning.org or telephone on 01934 313397 or by post at

13 Lime Close, Locking, Weston super Mare, North Somerset, BS24 8BH

It is important to note that whilst having a DPO in place can facilitate data compliance, DPOs are not considered personally responsible in the event of non-compliance with the GDPR. The responsibilities for any breach in GDPR compliance will always remain with ELAN as a whole.

Any serious breach of ELAN's data protection policy and privacy notices will be dealt with through the disciplinary policy and procedure.

7. Collecting personal data

We will only process personal data where we have a lawful basis for doing so under data protection law. The basis is limited to the following list:

- **consent** - the individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.
- **contract** - the data needs to be processed so that ELAN can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- **legal obligation** - the data needs to be processed so that ELAN can comply with a legal obligation
- **vital interests** - the data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- **public task** - the data needs to be processed so that ELAN can perform a task in the public interest, and carry out their official functions
- **legitimate interests** - the data needs to be processed for the legitimate interests of ELAN or a third party (provided the individual's rights and freedoms are not overridden)

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

8. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Employees will only process personal data where it is necessary in order to do their jobs. When employees no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with ELAN's data retention policy.

9. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- there is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- we need to liaise with other agencies – we will seek consent as necessary before doing this our suppliers or contractors need data to enable us to provide legitimate services to our staff and pupils for the efficient and proper running of our schools – for example, IT companies. When doing this, we will:
 - only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law
 - establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

- only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so for reasons, including, but not limited to:

- Workforce and School Census for the DfE
- pupil statutory assessment information for DfE
- pupil attendance data
- admissions data
- the prevention or detection of crime and/or fraud
- the apprehension or prosecution of offenders
- the assessment or collection of tax owed to HMRC
- in connection with legal proceedings
- where the disclosure is required to satisfy our safeguarding obligations
- research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Occasionally we may have to transfer personal data to a country or territory outside the European Union. In these situations, we will always inform you of our intention beforehand and will do so in accordance with data protection law, only after ensuring that appropriate safeguards are in place.

10. The right of access

Individuals have a right to make a 'data subject access request' (DSAR) to gain access to personal information that ELAN holds about them. This includes:

- confirmation that their personal data is being processed
- access to a copy of the data
- the purposes of the data processing
- the categories of personal data concerned
- who the data has been, or will be, shared with
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- the source of the data, if not the individual
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Data subject access requests should ideally be submitted in writing, either by letter or email or to the school or the DPO. They should include the following:

- name of the individual making the request
- name of the individual to whom the request for personal information relates
- correspondence address
- contact number and email address
- specific details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO. You should first ensure that the data requested is personal data relating to the employee. If it is not, for example, if it relates to profit data, then a data subject access request is not the appropriate method for a request and may be dealt with as a Freedom of Information request (FOI).

ELAN will verify the identity of the person making the request before any information is supplied. Individuals may be asked to provide two forms of identification.

It is a common misconception that employees have a right to see a copy of documents; this is not the case. They have a right see their personal data. However, a request is likely to be most easily dealt with by providing copies of documents. These may need to go through a process of redaction before being sent due to the potential identification of third parties.

All requests will be responded to without delay and at the latest, within one calendar month of receipt. However, in the event of numerous or complex requests, we may inform the individual that ELAN will comply within 3 calendar months of receipt of the request. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- might cause serious harm to the physical or mental health of the pupil or another individual
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- is contained in adoption or parental order records
- is given to a court in proceedings concerning the child.

ELAN will provide the information free of charge. However, where a request is manifestly unfounded or excessive, ELAN reserves the right to refuse to respond to the request or charge a reasonable fee which takes into account administrative costs. In the case of a refusal to respond to the DSAR, the individual will be informed of this decision and the reasoning behind it.

A request will be deemed to be manifestly unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain using the data protection complaints process which details escalation to the ICO (See appendix 1). A request may be manifestly unfounded if the following applies:

- the individual clearly has no intention to exercise their right of access - for example, an individual makes a request, but then offers to withdraw it in return for some form of benefit from the ELAN
- the request is malicious in intent and is being used to harass ELAN with no real purposes other than to cause disruption - for example, the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption
- the request makes unsubstantiated accusations against ELAN or specific employees
- the individual is targeting a particular employee against whom they have some personal grudge
- the individual systematically sends different requests to ELAN as part of a campaign, such as once a week, with the intention of causing disruption.

It will never just be assumed that the request is "manifestly unfounded". All requests will be considered carefully and in the context in which they are made. The use of the word

“manifestly” demonstrates that there is an obvious or clear quality to the request being unfounded. A genuine situation, where an individual wishes to exercise their rights, will not make the request unfounded.

Where a DSAR has been made electronically, the information will be provided in a commonly used electronic format. All fees will be based on the administrative cost of providing the information.

Children aged 12 or under are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

11. Additional rights in relation to data

Individuals also have additional rights in relation to data protection and any request to exercise these rights should be submitted to the DPO.

Any employee receiving such a request, should immediately forward it to the DPO.

Individuals have the following rights:

- to withdraw their consent to processing at any time
- In certain circumstances, to ask us to rectify, erase or restrict processing of their personal data, or to object to the processing of it
- To prevent use of their personal data for direct marketing
- challenge processing which has been justified on the basis of public interest
- request a copy of agreements under which their personal data is transferred outside of the European Union
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement), that might negatively affect them
- prevent processing that is likely to cause damage or distress
- be notified of a data breach in certain circumstances
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

12. Parental requests to see educational records

A request to see educational records should not be confused with a data subject access request. However, we would be happy to comply with such requests which should be directed to the DPO.

13. Privacy by design and privacy impact assessments

ELAN will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how ELAN has considered and integrated data protection into processing activities, including:

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- completing privacy impact assessments where ELAN's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- integrating data protection into internal documents including this policy, any related policies and privacy notices
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters and retaining records of the same
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- maintaining records of our processing activities

14. Data security

ELAN will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. This includes ensuring:

- paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal data are kept securely when not in use
- confidential paper records will not be left unattended or in clear view anywhere with general access or left anywhere else where access to them can be gained by unauthorised persons e.g. confidential documents left on a photocopier
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use
- Computers/laptops should be screen-locked when they are not in use (if not automatically locked)
- The use of Teams is encouraged for file sharing and storage within the organisation. This allows for monitoring of team memberships and access rights.
- passwords, which are complex, are used to access school computers, laptops and other electronic devices
- employees and where applicable, pupils are reminded to change their passwords at regular intervals
- All electronic devices are password-protected to protect the information on the device in case of theft
- USB devices used by staff must be issued by ELAN and encrypted
- employees or governors who store personal information on their personal devices are expected to follow the same security procedures as for ELAN-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected
- Documents in emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Sensitive or confidential information should not be shared in the body of an email.
- circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients

- where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, employees will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from ELAN premises accepts full responsibility for the security of the data which should be returned to ELAN as soon as practicable
- before sharing data, all staff members will ensure:
 - they are allowed to share it
 - that adequate security is in place to protect it
 - who will receive the data that has been outlined in a privacy notice
- under no circumstances should visitors be allowed access to confidential or personal information. Visitors to areas of the schools or other ELAN locations containing sensitive information must be supervised at all times
- the physical security of ELAN's buildings and storage systems, and access to them, is reviewed regularly and formally on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place

multi-factor authentication (MFA) is enabled where available. ELAN takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

15. Disposal of records

Personal data that is no longer needed will be disposed of securely in accordance with our data retention policy.

Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

We will shred paper-based records or use an approved external sensitive/confidential waste disposable provider, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on ELAN's behalf, but in this circumstance, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Data breaches

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

ELAN will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their professional development training, and will make all reasonable endeavours to ensure that there are no personal data breaches.

On finding or causing a breach, or potential breach, the employee or data processor must notify the DPO within 24 hours of discovery, who will alert the CEO if appropriate. Failure to report a breach may result in disciplinary action.

When appropriate, we will report the data breach to the ICO within 72 hours of being informed of the breach. Such serious breaches in a school context may include, but are not limited to:

- non-anonymised dataset being published on the school website
- safeguarding information being made available to an unauthorised person
- theft or hacking of a school laptop containing non-encrypted personal data about pupils and/or employees

- the school's cashless payment provider being hacked and parents' financial details stolen.

In the unlikely event of a suspected data breach, we will investigate the situation and determine whether a breach has occurred.

In order to make a decision, the DPO will consider whether the data has been accidentally or unlawfully: lost, stolen, destroyed, altered, disclosed or made available where it should not have been or made available to unauthorised people.

All reasonable efforts will be made by the DPO to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

All potential consequences will be assessed and dependent upon how serious they are, and how likely they are to happen, the DPO will work out whether the breach must be reported to the ICO or not. This will be judged on a case-by-case basis.

In reaching their decision, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress) as a result of:

- loss of control over their data
- discrimination
- identify theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation (for example, key-coding)
- damage to reputation
- loss of confidentiality
- any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO will notify the ICO, providing them with a description of the nature of the personal data breach, including the following, where known:

- the categories and approximate number of individuals concerned
- the categories and approximate number of personal data records concerned
- the name and contact details of the DPC
- a description of the likely consequences of the personal data breach
- a description of the measures that have been, or will be taken, to deal with the breach and to mitigate any possible adverse effects on the individual(s) concerned

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact.

If the risk is high, the DPO will, without undue delay, inform in writing, all individuals whose personal data has been breached. This notification will set out:

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

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

All breaches will be documented by the DPO, regardless of whether it is reported to the ICO, and will detail the facts including: the cause, the effects and any actions taken to contain it and ensure it does not happen again, such as establishing more robust processes or providing further training for individuals.

All records of breaches will be stored securely on ELAN's computer system, with limited access.

Following any breach, the DPO and CEO will meet as soon as reasonably possible, to review the circumstances of the breach and establish how this could be prevented from happening again.

Sensitive data – additional actions to be taken:

In the event that sensitive information is accidentally disclosed via email (including safeguarding records) to unauthorised users, every effort should be made to recall the email as soon as the error is realised.

Any employee who receives personal data sent in error, must alert the sender and the DPO as soon as they become aware of the error.

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT provider to recall it. Where this recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, to explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request and will carry out an internet search to check that the information has not been made public. In the event that it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

17. Publication of information

ELAN publishes information on its website that will be routinely made available, including:

- policies and procedures
- minutes of meetings
- annual reports
- financial information

ELAN will not publish any personal information, including photos, on its website without the permission of the affected individual, or a parent/guardian if the individual is a child.

When uploading information to ELAN websites, employees should be considerate of any metadata or deletions which could be accessed in documents and images on the site.

18. CCTV and photography

As part of our school activities, we take photographs and record images of individuals within our schools and when participating in school trips and visits. ELAN understands that recording images of identifiable individuals constitutes processing personal information. Therefore, it is done in line with data protection principles.

ELAN uses CCTV in various locations around some of its school sites to ensure the security of the premises and for the prevention and investigation of crimes.

We do not need to ask individuals' permission to use CCTV, but there are notices around the schools informing parents, pupils, employees, governors, suppliers/contractors and other visitors of the presence of CCTV.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for a maximum of thirty days for security purposes; Head Teachers are responsible for keeping the records secure and allowing access. Please refer to the CCTV Policy.

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

Consent for the taking, storing and use of images can be refused or withdrawn at any time. If consent is withdrawn, we will delete any relevant photographs or videos and not distribute it further.

We also sometimes use photographs and videos of pupils for communication, marketing and promotional materials. If ELAN wishes to use images/video footage of pupils in a publication, such as the school or ELAN websites, online on the schools' website and social media channels and outside of the schools, such as in publicity campaigns, prospectus, written permission will be sought for the particular usage from the parent of the pupil.

Precautions are taken when publishing photographs of pupils, in print, video or on the school/ or ELAN websites.

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

19. DBS data

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

Data provided by the DBS will never be duplicated.

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

20. Training

All employees and governors are provided with data protection training annually and as part of their induction process.

Data protection will also form part of professional development (PD), where changes to legislation, guidance or the schools' processes make it necessary.

21. Complaints

ELAN is committed to handling data protection complaints fairly and promptly. Individuals may raise concerns about any aspect of how their personal data is processed.

All complaints will be managed in accordance with our **Data Protection Complaints Process (Appendix 1)**, which sets out how complaints are submitted, handled, and resolved, including the right to escalate to the Information Commissioner's Office (ICO).

All staff must ensure complaints are recognised and escalated appropriately.

22. Policy review

The DPO is responsible for monitoring and reviewing this policy. The policy will be reviewed annually in line with the statutory recommendation.

The next scheduled review date for this policy is July 2027.

Appendix 1 – Data Protection Complaints Process

Purpose

This procedure sets out how we handle complaints relating to the processing of personal data, in accordance with UK data protection law.

Scope

This procedure applies to:

- All individuals whose personal data we process.
- All complaints relating to:
 - Data protection rights
 - Use of personal data
 - Data security
 - Subject access requests
 - Direct marketing or cookies

How to make a complaint

Individuals may raise a complaint through any of the following channels:

- **Email:** hr@extendlearning.org
- **Post:** Data Protection Officer, Extend Learning Academies Network, 13 Lime Close, Locking, Weston-super-Mare, BS24 8BH

Complaints can be submitted in any format and do not need to follow a specific template.

Logging and Acknowledgement

- All complaints will be recorded in the **Data Protection Complaints Log**
- We will acknowledge receipt of the complaint **within 30 calendar days**
- The acknowledgement will include:
 - Confirmation the complaint is being handled
 - Expected next steps
 - Contact details for follow-up

Investigation Process

We will:

1. Assess the nature and scope of the complaint
2. Identify relevant data processing activities
3. Review internal records, systems, and documentation
4. Speak with relevant staff where necessary
5. Assess compliance with UK GDPR and internal policies

Where needed, we may request further information from the complainant.

Response and Outcome

- We will respond without undue delay
- Our response will include:
 - A clear explanation of findings
 - Whether the complaint is upheld, partially upheld, or not upheld
 - Any actions taken or proposed

Where appropriate, we will:

- Correct or delete personal data
- Restrict or stop processing
- Update systems or processes
- Provide an apology or explanation

Timescales

- Acknowledgement: **Within 30 calendar days**
- Full response: As soon as reasonably possible (typically within **one/two months**, depending on complexity)

If more time is required, the complainant will be informed and given an updated timeframe.

Escalation and ICO Rights

If the complainant is not satisfied with our response, they have the right to escalate their complaint to the Information Commissioner's Office (ICO):

Website: <https://www.ico.org.uk>

Telephone: 0303 123 1113

We will inform complainants of this right in our response.

Record Keeping

We will maintain records of:

- All complaints received
- Actions taken
- Communications with the complainant
- Lessons learned and improvements made

Records will be securely stored and retained in accordance with our retention policy.

Continuous Improvement

We will regularly review complaints to:

- Identify patterns or recurring issues
- Improve processes and controls
- Enhance staff training and awareness

Responsibility

Overall responsibility for this process sits with:

ELAN Data Protection Officer

All staff are responsible for:

- Recognising potential complaints
- Promptly forwarding them to the appropriate contact