Laurel Avenue
Community Primary School

Data Protection Policy (GDPR) 2024

Introduction

Schools_and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not

- have permission to access that data,_and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in GDPR legislation and relevant regulations and guidance for the local authority, DfE and ICO.

1. Aims & Objectives

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- how staff, parents and pupils can access personal data.
- the rights in respect of people whose data is being held and processed by the school (this includes pupils, parents, staff and governors).

1.1. Safeguarding

The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.

Keeping children safe in Education

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

1.2. **It is a statutory requirement for all schools to have a Data Protection Policy:**

(http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools)

In addition to this policy, schools should have:

- **Retention Information** - details on how long all records are retained
- **Information Asset Audit** - a comprehensive audit listing all the information that the school holds, who has access to the information and the legal basis for processing it
- **Privacy Notices -** for pupils, parents, staff and governors
- **Registered with the ICO**

This policy will link with the following:

- Safeguarding Policy
- Staff AUP/Code of Conduct
- Photographic Policy
- Photographic Consent Forms

1.3. Data Protection Principles

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In Addition article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect the school, as the 'data controller', needs to be able to show that its policies and systems comply with requirements of GDPR.

2. Lawful Basis for processing data

GDPR stipulates that there must be a lawful basis for processing data, and that for special category data an additional condition has to be met. The vast majority of information that schools collect and process is required to enable the school to perform tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller. This is the main lawful basis for processing data that a school is likely to rely on.

There are other bases that may be available, such as a specific legal obligation applying to the data controller that makes the processing necessary. Your legal advisor will be able to identify individual statutes if required.

2.1 Age.

Children under the age of 13 are not usually considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians can do this on their behalf, providing this is in the best interests of the child. See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/
Children should be provided with age appropriate advice about how their data is used.

2.2 Consent. If there is a lawful basis for collecting data then consent to collect data is not required. (An employee could not opt to withhold an NI number for example.) However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 13) will be required. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or children over the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will need to be transparent, revocable, and will need to be on an "Opt-in" basis.

3. RIGHTS

The GDPR creates some new rights for individuals and strengthens some existing ones. It provides for the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

For "privacy notices" covering the right to be informed, please see section 5 below.

Different rights attach to different lawful bases of processing:

	Right to erasure	**Right to portability**	**Right to object**
Vital Interests	✓	X	X
Legal Obligation	X	X	X
Public Task	X	X	✓

Legitimate Interests	✓	X	✓
Contract	✓	✓	X
Consent	✓	✓	X but right to withdraw consent

The right to be informed – *See Privacy Notices section 6.2*

The right of access

Depending on the age of the pupil, there are two legal basis for pupils or parents to request access to their data – a Subject Access Request or a request under the 2005 Education Regulations.

Subject Access request under GDPR

GDPR gives individuals the right to access any data that an organisation holds on them. Normally this has to be completed within 30 days without charge. Further guidance is available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ Schools should be aware that guidance from the ICO highlights the rights of the child. *"Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond* *directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child."*

In maintained schools, parents have another statutory right to access their children's educational record

This is part of the Education (Pupil Information) Regulations 2005. This applies to all children under 16 years and has to be completed in 15 working days. See https://ico.org.uk/your-data-matters/schools/pupils-info/

Information which may be withheld

On some occasions records could contain information which ***"is likely to cause significant harm to the physical or mental health of the child or others",*** for instance, if a child makes a disclosure of abuse. In these circumstances, the data should not be released and the pupil/parent does not need to be informed of its existence. If in doubt seek legal advice.

The right to erasure

GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. Your legal advisor will be able to support with information about which data can continue to be legally held if a data subject asks to be 'forgotten'. Schools' data management systems such as SIMS will begin to improve their functionality to either delete or anonymise personal data when appropriate.

It will be seen from the table above that, where a school relies on either a 'legal obligation' or a 'public task' basis for processing (see above), there is no right to erasure – however, this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school's data retention guidelines.

It will be seen from the table above that where a school relies on either a 'legal obligation' or a 'public task' basis for processing (see above) there is no right to erasure – however this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school's data retention guidelines.

4. Data Types

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school data. GDPR defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a "Potential Data Breach" which could result in legal action against the school. The loss of sensitive, or "special category", *personal data is considered much more seriously and the sanctions may well be more punitive.*

4.1. Personal data

The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

4.2. Special Category Data

"Special Category Data" are data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive, and so needs more protection.

In a school the most likely special category data is likely to be:

- information on the racial or ethnic origin of a pupil or member of staff
- information about the sexuality of a child, his or her family or a member of staff
- medical information about a child or member of staff (SEND)
- (Some information regarding safeguarding will also fall into this category.)staffing e.g. Staff Trade Union details

Note – See section on sharing information.

4.3. Other types of Data not covered by the act

This is data that does not identify a living individual and, therefore, is not covered by the remit of the DPA - this may fall under other 'access to information' procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

The ICO provides additional information on their website. See http://ico.org.uk/for organisations/data protection/the guide/key definitions

5. Responsibilities

The Headteacher and Governing Body are responsible for Data Protection, they should appoint a Data Protection Officer to manage data.

5.1. Risk Management – Roles: *Data Protection Officer*

The school should have a nominated member of staff responsible for the management of data protection.

According to the ICO the minimum role will include:

- to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

In some schools other staff may have been delegated responsibility for particular issues, for instance the handling of SEND information.

The school will identify these as Mrs S Snow, Admin Officer; Mrs M Angus, Admin Officer; Ms G Davison, Headteacher, Mrs S Tew (SENDCo) for the various types of data being held (e.g. pupil information/staff information etc.).

The DPO and persons with delegated responsibility will manage and address risks to the information and will understand:

- ♦ what information is held, for how long and for what purpose
- ♦ how information has been amended or added to over time, and
- ♦ who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

5.2. Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.

- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

5.2.1 Risk Assessments

Information risk assessments will be carried out by the DPO at the time of implementation of GDPR for all current systems and on the introduction of new systems, to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- ♦ Recognising the risks that are present
- ♦ Judging the level of the risks (both the likelihood and consequences) and
- ♦ Prioritising the risks.

Risk assessments are an on-going process and should result in the completion of an entry in the Information Asset Register.

5.2.2 Impact Levels and protective marking

Following incidents involving loss of data, the Government published HMG Security Policy Framework [http://www.cabinetoffice.gov.uk/spf], which recommends that the Government Protective Marking Scheme is used to indicate the sensitivity of data.

The *HMG Security Policy* recommends that the Government Protective Marking Scheme is used to indicate the sensitivity of data. The scheme is made up of five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most learner or staff personal data that is used within educational institutions will come under the PROTECT or RESTRICTED classifications.

To ensure a uniform method of assessing the impact of potential compromises to the confidentiality, integrity or availability of information and information systems, and provide comparable levels of information protection when the data is shared, Business Impact Levels tables have been devised. All data – electronic or on paper – should be labelled according to the protection it requires, based on these Impact Levels. Impact Levels 2 -6 correspond to the adjectival descriptions PROTECT to TOP SECRET.

The following table illustrates the assignation of Impact Levels for Distress to the Public.

Impact Level 1	**Impact Level 2**	**Impact Level 3**	**Impact Level 4**
Not Protectively Marked	Protect	Restricted	Confidential*

Impact Level 1	Impact Level 2	Impact Level 3	Impact Level 4
None	Likely to cause embarrassment to an individual or organisation	Likely to cause loss of reputation to an individual or organisation	Likely to cause embarrassmen or loss of reputation to many citizens or organisations

*Confidential, Secret and Top Secret are not applicable in a school setting

Impact Level	Example Data Types
IL0/IL1	• Google search results • BBC News
IL2 – PROTECT	• General student data • Learning platforms/portals
IL3 – RESTRICTED	• School MIS (eg SIMS data) • Teacher access to learning platform/porta • Special educational needs • Pupil characteristic • Health records
IL4 - CONFIDENTIAL	• National Pupil Database • Looked-after children • Witness protection

Impact Level	Example Data Types
	• SEN IL4 data elements

The person writing a document is responsible for applying the correct protective marking. They do this by clearly labelling each page of a document, normally in the footer, with the correct marking.

When protectively marking a document, it is recommended that a damage or 'harm test' is conducted to consider the likely impact if the asset were to be compromised and to help determine the correct level of marking required.

If applied correctly, the Protective Marking System will ensure that only genuinely sensitive material is safeguarded. Be aware that applying too high a protective marking can inhibit access and impair efficiency while applying too low a protective marking may lead to damaging consequences and compromise of the data.

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.
The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to and the handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

Users must be aware that when data is aggregated, the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. 'Securely delete or shred this information when you have finished using it'.

5.3 Training and Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff Meetings/Professional Development Sessions
- Day to day support and guidance from DPO

5.4 Home Working/Learning

In certain circumstances staff /pupils may be required to work/access learning from home. In such circumstances all GDPR principles/procedures are adhered to and followed as per school/legal requirements.

Provision for staff:

- HT and DHT have secure school laptops

- Staff use password secured, school approved USB sticks
- Staff use password secured, school i-pads which are signed out of school when necessary
- Staff have access to GDPRis for reporting, advice and guidance
- Staff share documents using secure email and school one drive
- Children's books are to remain in school due longer, enforced periods of home learning
- System in place to recover children's books in a timely manner should a member of staff have to begin working from home without notice

Provision for Pupils:

- Use of Office 365 logins for secure access to online lessons and learning; email
- Secure school platform through Class Dojo for submitting home learning and corresponding with class teacher.

Provision for Parents:

- Secure school platform through Class Dojo for corresponding with class teacher
- Use of email to correspond with school office HT and DHT.

6. Legal Requirements

6.1. Registration

The school must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration: https://ico.org.uk/for-organisations/data-protection-fee The register may be checked by visiting https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

6.2. Information for Data Subjects (Parents, Staff): PRIVACY NOTICES

In order to comply with the fair processing requirements of the DPA, the school **must** inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc) to whom it may be passed. The privacy notice will also need to set out the data subjects' rights under the GDPR. This privacy notice will be passed to parents / carers through a letter. More information about the suggested wording of privacy notices can be found on the DfE website: http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn

Updated privacy notices are issued to all 'data subjects' even if the data subject has previously received a similar notice. This is because of the new rights in the GDPR that people should be informed about.

(see school **Privacy Notice)**

Children are be provided with age appropriate information about how their data is being used.

7. Transporting, Storing and Disposing of personal Data

7.1. Information security - Storage and Access to Data

The more sensitive the data the more robust the security measures will need to be in place to protect it.

7.1.1. Technical Requirements

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes. (see school policy: **Password Security**)

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

(see school policy: **Secure storage of and Access to Data Policy**)

Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data. (see school policy: **Secure Storage of and Access to Data Policy**)

The school / academy has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (see school policy**: Automatic Backup Systems**) **LINK TO WEBSITE WILL BE ADDED**

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
- the school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices
- Only encrypted removable storage purchased/approved by the school is allowed to be used on school computers and these are not functional with scanners.

(see school policy: **Portable Devices and Removable Media Section of Secure storage of and Access to Data Policy**)

7.1.2. Passwords

All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded. (see school policy: **Password Security**)

7.1.3. Images

- Images of pupils will be collected, stored and shared in accordance with the School Photographic Policy and, Secure Storage and Cloud Based Systems Policies.
- (see school policy: **School Photographic Policy**)

7.1.4. Cloud Based Storage

- The school / academy has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Google Apps and Onedrive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. See advice from the DfE below:-

- ○ https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

7.2 Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home),they should have secure remote access to the management information system or learning platform, Durham Learning Gateway
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local

authority (if relevant) in this event. (nb. to carry encrypted material is illegal in some countries)

7.3 Third Party data transfers

As a Data Controller, the school / academy is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party as well as data processing agreements.

http://ico.org.uk/for organisations/data protection/topic guides/data sharing

7.4Rention of Data

The guidance given by the Information and Records Management Society – Schools records management toolkit can be used as a basis for determining how long records are kept. This school retention information should be available to data subjects on request.

Systems to protect data

7.4.1Paper Based Systems

- All paper based personal data will be protected by appropriate controls, for example:
  - Paper based safeguarding chronologies will be in a locked cupboard when not in use
  - Class Lists used for the purpose of marking may be stored in a teacher's bag.
- Paper based personal information sent to parents (will be checked by ..., before the envelope is sealed).
- Passwords are used to secure print jobs of data such as performance data and all special category data, for example SEND, Medical.

7.4.2 School Websites

- Uploads to the school website will be checked prior to publication, for instance:
  - to check that appropriate photographic consent has been obtained
  - to check that the correct documents have been uploaded.

7.4.3 E-mail

> *E-mail cannot be regarded on its own as a secure means of transferring personal data.*

Where technically possible all e-mail containing sensitive information will be encrypted by *(…for instance* … by attaching the sensitive information as a word document and encrypting the document / compressing with 7 zip and encrypting. The recipient will then need to contact the school for access to a one-off password) or using the security features available in Office 365.

7.4.4 Admin and Curriculum Servers

All data should be backed up according to its value to the Institution, the cost of recreating the data, any financial costs or penalties which might be incurred as a result of data loss or corruption, and the risk of data loss or corruption.

The purpose of data backup is purely to allow the Institution to continue its activity after a data loss incident, by retrieving some or all of the data lost, ideally from a point in time backup taken within the last 24 hours.

The school has clear policy and procedures for both the protection against virus and other threats including the use of PANDA anti-virus software and automatic backing up, accessing and restoring all data held on school systems, both on and off-site. backups. (see **Automatic Backup Systems Policy**) **LINK TO WEDSITE WILL BE ADDED**

6.4 Disposal of Data

- The school will comply with the requirements for the safe destruction of personal data when it is no longer required.
- The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded or otherwise disintegrated for data.
- A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

8 Data Sharing

8.Sharing with the LA and DfE

The school is required by law to share information with the LA and DfE. Further details are available at: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

8.1Safeguarding

Schools MUST follow the statutory processes in Keeping Children safe in Education and Working together to Safeguard Children https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Durham LSCB provides information on information sharing at: http://www.durham-lscb.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

8.2 Transfer of Safeguarding and SEND records when a pupil moves school

The following is an extract from keeping Children safe in Education Sept 2018.

- Where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, ensuring secure transit, and confirmation of receipt should be obtained. For schools, this should be transferred separately from the main pupil file.

- Receiving schools and colleges should ensure key staff such as designated safeguarding leads and SENCOs or the named person with oversight for SEN in a college, are aware as required.

- In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any information with the new school or college in advance of a child leaving. For example, information that would allow the new school or college to continue supporting victims of abuse and have that support in place for when the child arrives.

9 Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach, the data protection officer will inform the head teacher and chair of governors.
- When a personal data breach has occurred, the school must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely then you don't have to report it. However, if the school decide not to report the breach, they need to be able to justify this decision, and it should be documented.
- The school must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If the school takes longer than this, they must give reasons for the delay.
- If a breach is likely to result in a high risk to the rights and freedoms of individuals, GDPR states you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

Any report about a data breach must include:

- a description of the nature of the personal data breach including, where possible:

    - the categories and approximate number of individuals concerned; *and*
    - the categories and approximate number of personal data records concerned;

- the name and contact details of the data protection officer or other contact point where more information can be obtained;

- a description of the likely consequences of the personal data breach; *and*
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects.

Further details are available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

10 Freedom of Information Act

Laurel Avenue Community Primary School has a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy the school should:

- Delegate to the Headteacher day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy.
- Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need.
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body.
- Proactively publish information with details of how it can be accessed through a Publication Scheme and review this annually.
- Ensure that a well-managed records management and information system exists in order to comply with requests.

(see school policy: **Freedom of Information**)

http://fluencycontent2-schoolwebsite.netdna-ssl.com/FileCluster/LaurelPrimarySchool/MainFolder/Content/Documents/Policies/Freedom-of-Information-2017.pdf

Policy Review Reviewing:

This policy will be reviewed, and updated if necessary every two years or when legislation changes.

Date: September 2023 Review: September 2024

Signed:

Chair of Governors

Adopted by the Governing Body on ________________

The Data Protection Officer is Mrs Helen Walters (Deputy Headteacher)

Appendix 1 - Links to resources and guidance

ICO Guidance on GDPR

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

http://ico.org.uk/for organisations/sector guides/education

Specific information for schools is available here. This includes links to guides from the DfE

http://ico.org.uk/for organisations/data protection/topic guides/cctv

Specific Information about CCTV

Information and Records Management Society – Schools records management toolkit

http://irms.org.uk/page/SchoolsToolkit

A downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS)

https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information

Details of storage and access to DBS certificate information.

DFE Privacy Notices

https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

DFE Use of Biometric Data

https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Appendix 2 - Privacy Notices

These are now a separate attachment

Appendix 3 - Glossary

GDPR - The General Data Protection Regulation. These are new European-wide rules that are the basis of data protection legislation. They are enforced in the UK by the ICO.

Data Protection Act 1998: Now superseded by GDPR

All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO:

The Information Commissioner's Office. This is a government body that regulates the Data Protection Act and GDPR

The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England:

General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media:

General information note from the Information Commissioner on publication of examination results.

Education Act 1996:

Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005:

Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972: Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998:

Retention of school admission and exclusion appeal papers and other pupil records.

Appendix 4 - Check Sheet

Schools may find it beneficial to use this to check their systems for handling data.

- □ Data protection Officer in place
- □ Information asset log complete
- □ School able to demonstrate compliance with GDPR
- □ Training for staff on Data Protection, and how to comply with requirements
- □ Data Protection Policy in place
- □ All portable devices containing personal data are encrypted
- □ Passwords – Staff use complex passwords
- □ Passwords – Not shared between staff
- □ Privacy notice sent to parents/pupils aged 13 or over
- □ Privacy notice given to staff
- □ Images stored securely

□ School registered with the ICO as a data controller

□ Systems in place to ensure that data is retained securely for the required amount of time

□ Process in place to allow for subject access requests

□ If school has CCTV, appropriate policies are in place to cover use, storage and deletion of the data, and appropriate signage is displayed

□ Paper based documents secure

□ Electronic backup of data both working and secure

□ Systems in place to help reduce the risk of a data breach *e.g. personal data sent out checked before the envelope sealed, uploads to websites checked etc*