Our Vision: "To make every day count"

Data Protection Policy

General Data Protection Regulation (GDPR)

Head Teacher: Mrs Catherine Dennison

Signed:_____

Chair of Governors: Mr Kevin Porter

Signed:

Date:

Review Date: Annually

Edited by:	Catherine Dennison - Headteacher Denise King – School Business Manager	
Read and agreed and proposed by:	Policy Sub-Committee Rachel Sheard Mark Readhead Denise Burness Donna Loftus Kevin Porter	
Considered and ratified by:	Kevin Porter – Chair of Governors	

At Black Combe Junior School we adopt Cumbria County Council's Policy for GDPR and Data Protection. This policy is their latest update with additional Black Combe Junior School relevant information.

Cumbria County Council

Cumbria County Council

General Data Protection Regulation (GDPR)
Guidance for Schools

February 2018

Contents

Some basics….

Nine out of ten Europeans have expressed concern about mobile apps collecting their data without their consent, and seven out of ten worry about the potential use that companies may make of the information disclosed.

Schools hold an increasing amount of personal data as service providers and employers and can assume that if the data held falls within the scope of the DPA, it will also fall within the scope of the GDPR.

In January 2012 the European Commission began work on a new legislative framework for data protection. The General Data Protection Regulation (GDPR) came into force on 24 May 2016. There is two-year transition period for implementation, so that the new rules, as incorporated in the Data Protection Bill, will come into force on 25 May 2018.

The Data Protection Bill incorporates the GDPR directly into UK law. The GDPR promises to update and modernise the principles enshrined in the 1995 Data Protection Directive (and consequently the Data Protection Act 1998) to guarantee privacy rights. It focuses on:

- reinforcing individuals' rights
- strengthening the EU internal market
- ensuring stronger enforcement of the rules
- streamlining international transfers of personal data and
- setting global data protection standards.

It applies to both digitally stored data and to records held in other forms

Within this framework, the aim is to give people **more control** over their personal data and make it easier to access, and so build trust. The rules are designed to make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU, as may often be the case on the internet.

Personal Data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal Data

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Introduction

Data Protection governs how information about living people (such as pupils and staff) is collected and used. The current legislation (Data Protection Act 1998) came into force almost 20 years ago and it has long been recognised that it needed to be updated given the way technology – particularly the internet – has developed.

The result is the General Data Protection Regulation (GDPR), which becomes law on **25 May 2018.**

The GDPR is a major piece of legislation and there are some important changes to the current Act, including the headline-grabbing aspect that the size of potential fines is significantly increasing (from £500,000 up to €20,000,000).

However, GDPR is predominantly taking what is current best practice and making it a legal requirement. In other words, it's more prescriptive on what we have to do than the current Act.

GDPR applies to all organisations (not just public sector) and we are all in the same boat in terms of understanding the new legislation.

The Information Commissioner's Office (ICO), recognises this and has recently made a statement to say that in order to comply with the General Data Protection Regulation (GDPR) organisations should be putting key building blocks in place to ensure improvements in data protection practices.

These include:

- Organisational commitment – preparation and compliance must be cross-organisational, starting with a commitment at Governor level. There needs to be a culture of transparency and accountability as to how you use personal data – recognising that the public has a right to know what's happening with their information.
- Understand the information you have – document what personal data you hold, where it came from and who you share it with. This will involve reviewing your contracts with third party processors to ensure they're fit for GDPR.

- Implement accountability measures – including appointing a data protection officer if necessary, considering lawful bases, reviewing privacy notices, designing and testing a data breach incident procedure that works for you and thinking about what new projects in the coming year could need a Data Protection Impact Assessment.
- Ensure appropriate security – you'll need continual rigour in identifying and taking appropriate steps to address security vulnerabilities and cyber risks
- Train Staff – Staff are your best defence and greatest potential weakness – regular and refresher training is a must.

This guidance is designed to explain the key things you need to have in place by 25 May 2018. It looks at what you may already have, and what's needed to upgrade it to GDPR standards.

If you already have good policies and practices in place, it will largely be a case of making some changes and adding to what you've got. If you're a bit further behind then there will be more work to do to catch up.

The Information Commissioner's Office (ICO) has produced a range of guidance to help you understand your obligations:

- Data Protection for the Education Sector: https://ico.org.uk/for-organisations/education/
- Guide to the General Data Protection Regulations https://ico.org.uk/for-organisations/data-protection-reform/
- Frequently Asked Questions – Education Sector https://ico.org.uk/for-organisations/education/education-gdpr-faqs/

The County Council also offers a traded service to schools for legal advice that covers the Data Protection Act and Freedom of Information Act. To find out more about this service please visit:

Website: Traded Services

Email: TradedServices@cumbria.gov.uk

Telephone: 01228 226817

Task 1: Registration

Schools, as with most other organisations that use personal data, must register with the Information Commissioner and pay the relevant fee.

GDPR will have an impact on registration so from May 2018, whilst you won't need to register in the same way you will still have to pay a fee.

The Information Commissioner is currently consulting on the fee structure but the draft proposal suggests that the fee payable by schools may increase slightly to £55 (other organisations will be more, up to £1,000).

If you are already registered then you don't need to take any further action for now but you will still need to pay your annual fee. You can monitor the conversation with regard to fees at: https://iconewsblog.org.uk/

Black Combe Junior School		
Action:	Who?	Date:
Register with information Commissioner	Denise King - SBM	

Task 2: Information Asset Register

This ties in with accountability and is one of the key documents to show that you are complying with the GDPR. To manage data effectively you need to know what key types of data you've got, what you use it for, and how you should be looking after it. This is what's recorded in your Information Asset Register (IAR). It's a list of the main types of information you have, stating for each one key details such as why you have it, what you use it for, where it's stored, who it is shared with (if it is) and how long you keep it for.

You probably won't have an IAR currently, but you'll already know most of the key information that you hold and need to record, even if you haven't documented it formally.

It would be a good idea to use your existing ICO registration as the basis for your IAR – an example is included in Appendix 1.

As previously mentioned you won't need to register in the same way in future, what this means is that rather than record that detail on your ICO registration, you need to document the records you hold and why you use them so they can be provided if requested (by the ICO or anyone else).

Black Combe Junior School			
Action:	Who?	Where?	Updated:
Information Asset Register	Denise King - SBM		

What do I need to do?

You should consider doing an information audit to identify the records you hold and start to create your IAR and keep it up to date. As a starting point use the template published by the ICO.

Task 3: Privacy Notices

Privacy notices are what we use to explain to pupils, parents and employees why we collect information and what we're going to do with it, such as if we're going to share it with anyone else. You need to ensure you have them (note that GDPR increases the amount of detail you need to include) and they are made available to the people whose data you collect.

Details that need to be covered in a privacy notice:

- the school's name and contact details
- contact details of the data protection officer
- the right to complain to the ICO
- why you are processing the personal data and the legal basis for the processing
- details of any other organisations you may share the data with
- details if you intend to transfer the data to another country
- how long the data will be stored for, or the criteria it would be based on (retention schedule etc)
- whether they need to provide personal data based on a statutory or contractual requirement,
- that they can withdraw consent at any time
- if there will be any automated decision-making, including profiling, and that they have the right to meaningful information about the logic involved
- their various rights around their data: the right to request access to a copy, to request that it is rectified or erased, to restrict processing, to object to processing, to receive data in a portable format.

Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand.

What do I need to do?

Check if you've got notices already and how you make them available to parents, pupils and employees (typically on your website).

A sensible starting point if you do not have a privacy notice is your registration document. You can find this by going to https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/ and inserting the name of your school. An example is included at Appendix 1.

You can also use the examples created by the Department for Education although significant work will be required to populate these templates.

Think about how you can provide this information – not just on your website but in printed format for those who do not have access to online services.

Black Combe Junior School			
Action:	Who?	Where?	Updated:
Privacy Notice - Employees	Denise King - SBM		
Privacy Notice - Parents	Denise King - SBM		
Privacy Notice - Children	Denise King - SBM		
Website	Denise King - SBM		

Task 4: Protecting Children Online

Safeguards for children are made up of two basic elements, an age limit on consent to personal data processing, and a clearer right to be forgotten.

The GDPR includes a requirement for parental consent to personal data processing on behalf of young children using information services, and allows the threshold to be set nationally, to any age between 13 and 16 years. Currently there are no overall rules, although the Information Commissioner recommends safeguards until 12 years.

The threshold of 13 years has been adopted for the UK. The aim is to protect children from being pressurised into share personal data without fully realising the consequences, without stopping teenagers from using the Internet to get information, advice, or education.

Significantly, the rules specify that the consent of the holder of parental responsibility should not be necessary for preventive or counselling services offered directly to a child.

There is an additional safeguard. When children have made data about themselves accessible – often without fully understanding the consequences – the GDPR makes clear that they must not be stuck with the consequences of that choice for the rest of their lives.

This will be of particular relevance for social media platforms, and other uses of the

Internet. In line with the main provision for erasure, this will not be an absolute right, but is one that will be widely welcomed.

What do I need to do?

Understand the services you are providing to children and ensure that the relevant consents are in place if required.

Black Combe Junior School			
Action:	Who?	Where?	Updated:
Trips			
Images			
Pain Relief			
Permissions update at first Parent Evening (October) MIS: ScholarPack updated at this time. See Consent Form at Appendix 2			

Task 5: Consent

GDPR strengthens the rules when it comes to when you can rely on consent and what you need to do as part of getting and recording consent. When you seek consent, you must make it completely clear what they are consenting to, their consent must be unambiguous (positively opting-in) and you must make them aware they can withdraw their consent at any time.

The crucial point with this is that it only relates to getting consent to collect, record and use personal data. This doesn't affect any other situations where you may seek consent to do something.

You'll already have processes around how you collect and use personal info and you may currently ask for consent in some cases as part of doing that. If so, you'll have some existing wording (on a form etc) around how you ask for that consent.

Most of what you collect and use personal data for is linked to your statutory responsibilities around education provision or your role as an employer. In those cases, you don't need to ask for consent, you just have to explain why you need the information and/or why you need to use the information (done via the Privacy Notices mentioned above). So, if you're currently seeking consent in those situations you'll need to revise that process along those lines.

What do I need to do?

If you do anything that isn't covered by your statutory responsibilities then you'll need to consider how you go about asking for consent. It needs to be completely clear what they are consenting to, offer them a free choice to give their consent, they need to opt in to it (opt-out boxes are not allowed etc) and you should make clear that they can withdraw their consent at any time (and how to do this).

Task 6: Data Protection Officer (DPO)

Under the GDPR, you **must** appoint a DPO if you:

- are a public authority (except for courts acting in their judicial capacity);
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

Maintained schools are public authorities as defined by Schedule 1[1] of the Freedom of Information Act 2000. The ICO defines this further[2] "within the education sector, it is the governing body of a school, further education institution or university that is the public authority".

Black Combe Junior School's Data Protection Officer is

Catherine Dennison and is supported by Denise King and Ruth Farquhar.

(SBM and Office manager)

A single data protection officer can act for a group of schools, taking into account their structure and size.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

The DPO's main tasks are:

- to inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws (such as when using a new IT system, and responding to requests and complaints)
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train employees and conduct internal audits.
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

What do I need to do?

Your school might already have someone who looks after information governance issues so it would make sense for them to take the lead and act as the Data Protection Officer. It is important to remember that in the event of a data breach, someone with

[1] http://www.legislation.gov.uk/ukpga/2000/36/schedule/1
[2] https://ico.org.uk/media/for-organisations/documents/1152/public_authorities_under_the_foia.pdf

local knowledge of the school, how it works, where its information is stored and how to contact key members of staff will need to take the lead on any investigations.

When you have decided who will perform this role their contact details will need to be made available to anyone that needs them, for example including them on your privacy notices.

Task 7: Rights

As with the DPA, the GDPR give individuals various rights around their data:

- Right of access (to receive copies of their personal data)
- Right to rectification (correcting data if inaccurate)
- Right to erasure (to request that data is deleted)
- Right to restrict processing (to request you don't use their data in a certain way)
- Right to data portability
- Right to object
- Right to have explained if there will be any automated decision-making, including profiling, based on the data and that they have the right to meaningful information about the logic behind this.

The main one is being able to request a copy of the information you hold about them, but it also gives them the right to do things like request that information is corrected (if inaccurate).

The general scope of the rights are similar to those currently within the DPA, but GDPR is stricter on what you need to do (for example, having 'one month' to reply to a request rather than 40 days).

The key changes for this area are:

- in most cases you will not be able to charge for complying with a request (currently you can charge up to £10).
- you will have a month to comply, rather than the current 40 days.
- you can refuse or charge for requests that are manifestly unfounded or excessive.

Most of the rights people have under GDPR they already have under the Data Protection Act, so chances are you already have some experience in dealing with any requests, even if you don't have a formal procedure.

What do I need to do?

Understand what rights people have and put a process in place for how you will handle any requests you receive. If you've already got a process then be aware that GDPR does change some of the requirements, so you may need to revise them. The main type of request you'll get is when a pupil, or a parent or guardian with parental responsibility, asks for a copy of the information you hold about them.

Task 8: Data Breaches

Under GDPR, a serious breach (based on the amount and sensitivity of data lost) must be reported to the ICO within 72 hours. In those cases, you would also be required to inform the people whose data has been compromised (lost, sent to the wrong person etc) about what has happened.

Whilst there is no mandatory requirement to report a breach under the DPA, if one was reported – either by an employee, parent or pupil - then action had to be taken to contain it. Put simply you needed to:

- investigate to understand what has happened;
- act to put it right where possible (i.e. if you sent a letter to the wrong person, contact them to get it back);
- identify/communicate if there are any actions or lessons learned to prevent reoccurrence.

The ICO will be issuing guidance in the coming months to explain which breaches they would expect to be notified of. This is likely to be based on the sensitivity and volume of information breached and the potential impact this could have on the person/people it is about.

If the data is relatively basic (name/address etc) and there is little risk of it being used (information has been retrieved, was accidentally sent to a professional etc) then, whilst you still would need to log and investigate it, you probably wouldn't need to report to the ICO.

If the data was more sensitive (medical information etc) and there is a risk it could be further shared (you don't know who has got it, it was wrongly emailed to lots of people etc) then that type of case would likely need to be reported.

What do I need to do?

You should identify if you have a Data Breach Reporting Procedure – if you have update it and ensure all employees are aware of it, if you haven't further details can be found on the ICO website: https://ico.org.uk/for-organisations/report-a-breach/

Task 9: Data Protection Impact Assessments (DPIAs)

Currently, if you were planning a major change to how you use personal data (for example, moving to a new IT system, or perhaps a merger of two or more schools), you should do a risk assessment so that you spot the potential risks to the data and ensure things are put in place to mitigate. GDPR calls that a DPIA and makes it a requirement to do one in some cases (again, essentially where there's a lot of data involved and/or particularly sensitive data).

Currently they are referred to as Privacy Impact Assessments so you may have heard of them before, but you may not have used them much at all in a formal sense. However, mostly it's about common sense and thinking things through properly when proposing to change something, so you're probably doing it already in one form or another.

What do I need to do?

For your purposes, currently you just need to be aware of this so that you spot when such a situation crops up and can then look at the guidance on the ICO's website (which includes template assessment forms) to complete the assessment when needed.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

Task 10: Contracts

If you are entrusting another organisation with personal data (HR provider, IT company, someone providing alternative education etc) then you need to make sure they will manage that information responsibly by virtue of what you have in your contracts with them. GDPR increases the liability on third parties you have contracts with and also puts you under greater responsibility to ensure the third party will handle personal data securely.

If you have any contracts with anyone that involve them using your school's personal data (staff info, pupil info etc), those contracts should already have some wording in there covering responsibilities on complying with DPA, keeping info secure and confidential etc.

What do I need to do?

The ICO has recently published some draft guidance on what needs to be included in contracts. At this stage, the main thing is to be aware of what contracts you have

(should come up in your IAR) and be prepared that some wording changes may be needed based on the final version of the ICO's guidance. From a school's perspective, it's possible that your contractors will take the lead on updating contract terms, but keep it in mind.

https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/consultation-on-gdpr-guidance-on-contracts-and-liabilities-between-controllers-and-processors/

Task 11: Security

Some school records will be on paper, but most will be stored in databases and other computer systems. The cases that hit the headlines (and attract the fines) are those where large volumes of personal data have been lost, destroyed or stolen from digital systems.

Most of what follows is simply good practice, but as recent cases show, this isn't being followed, even by large corporations with dedicated technical teams. However, most schools will already comply with the majority of this if they have good technical support.

The following checklist will help you to ensure you have sensible technological measures in place to keep data safe.

Technological measures	BCJS	Date	Who
Backups – are they being done regularly by you and your suppliers?	System IT	Daily to the cloud	
Access controls – • Are adequate protective measures in place such as strong passwords? • Are all devices that access school data (laptops, tablets and smartphones) also adequately protected? • Does your procedure for leavers ensure their access rights are revoked?			
Encryption – any device that stores the school's data should be encrypted.			
Physical security - Most schools use a range of devices to access their systems. If they're portable are they kept securely when not in use?			
Antivirus and patching –			

All devices should have up-to-date antivirus software and be updated with all recent "patches".			
Attack from the internet. If your school is on CPSN, then there are already adequate measures to make it difficult for intruders to access your systems from the internet. However, if you buy your internet services direct from a third party you will need to ensure they have a credible statement about issues like firewalls and penetration testing.			

Task 12: Training

GDPR is going to increase scrutiny on how you comply with Data Protection.

What do I need to do?

Employees don't need to know the legislation back to front, but just make sure to remind them on a periodic basis going forward (one a year etc) of the key things around keeping information secure and knowing who to raise anything with if they think there's an issue.

Black Combe Junior School			
Action:	Who?	When?	Updated:
ECT / New Staff Training	CLD	As and when needed	
Annual review of procedures	CLD, DAK, RF	Annually September	
Annual review of procedures for staff	All staff	Annually September	

Review: Compliance Checklist

Use the checklist below to assess your current practices under the Data Protection Act 1998.

Completed: January 2023

Question	Yes	No	Comments
Is your school registered with the Information Commissioner?	☒	☐	
Does your school have an Information Asset Register?	☒	☐	
Is your school considering doing an information audit?	☐	☐	
Does your school have a retention schedule?	☐	☐	
Has your school reviewed its Privacy Notices – including how, where and when they are communicated to pupils, parents and employees?	☐	☐	
Does your school provide any information society services to children?	☐	☐	
Has your school reviewed where it currently asks for consent to collect and use personal data?	☐	☐	
Does your school need a Data Protection Officer?	☒	☐	
Does your school have an application process in place to support the rights outlined in Task 7?	☐	☐	
Has your school got a procedure in place for recording/reporting data breaches?	☐	☐	
Has your school got a procedure in place for conducting Data Protection Impact Assessments?	☐	☐	
Have you reviewed your data processor contracts?	☐	☐	
Have you reviewed your data security arrangements?	☐	☐	

Do you provide your employees with data protection/security awareness training?	☐	☐	

Appendix 1 - ICO Registration Form

Data Protection Register - Entry Details

Registration Number:
Date Registered:
Registration Expires:
Data Controller:
Address:

This data controller states that it is a public authority under the Freedom of Information Act 2000 or a Scottish public authority under the Freedom of Information (Scotland) Act 2002

This register entry describes, in very general terms, the personal data being processed by:

Nature of work - School

Description of processing

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

Reasons/purposes for processing information

We process personal information to enable us to:

- provide education, training, welfare and educational support services
- administer school property
- maintain our own accounts and records
- carry out fundraising
- support and manage our employees

We also use CCTV systems to monitor and collect visual images for security and the prevention of crime.

Type/classes of information processed

We process information relating to the above reasons/purposes. This information may include:

- name and personal details
- family, lifestyle and social circumstances
- financial details
- education details
- employment details
- student and disciplinary records
- vetting checks
- goods and services
- visual images, personal appearance and behaviour

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature
- trade union membership
- sexual life
- offences and alleged offences

Who the information is processed about

We process personal information about:

- our students and pupils
- advisers and other professional experts
- school staff
- members of school boards
- donors and potential donors
- suppliers
- complainants and enquirers
- individuals captured by CCTV images

Who the information may be shared with

We sometimes need to share the personal information we process with the individual themself and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- education, training, careers and examining bodies
- school staff and boards
- family, associates and representatives of the person whose personal data we are processing
- local and central government
- healthcare professionals
- social and welfare organisations
- police forces
- courts
- current, past or prospective employers
- voluntary and charitable organisations
- business associates and other professional advisers
- suppliers and service providers
- financial organisations
- security organisations
- press and the media

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the data protection act.

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK Data Protection Law

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

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR

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.

TERM	DEFINITION
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 Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation
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 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

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 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 provide an annual report of their activities directly to the governing board and, where relevant, report to the board 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.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Denise King and is contactable via the school office on 01229 772862.

5.3 Headteacher

The Headteacher (Catherine Dennison) acts as the representative of the data controller on a day-to-day basis and has overall responsibility. The Headteacher works closely with the DPO.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With 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
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say 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 school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 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.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they **must** ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 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 school 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data 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 (see section 6)

- Completing data protection impact assessments where the school'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; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

13. Data security and storage of records

We 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.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-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 (see section 8)

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. 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.

15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

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

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

16. Training

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

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every year and shared with the full governing board.

18. Links with other policies

This data protection policy is linked to our:

Freedom of information publication scheme

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by email as soon as possible.

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Headteacher and the chair of governors

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - 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 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 breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay,

the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- 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 consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the school secure files.

The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

The DPO and Headteacher will meet regularly (at least once per term) to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive 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 System IT to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, 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 endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupil or families