Abbotskerswell Primary School

Data Protection Policy

This Policy was adopted by governors:

Version date: 17th Oct 2019 Review date: October 2021

For further information on the retention of school data, please follow the link below.

https://new.devon.gov.uk/keepingdevonsdata/education-and-learning/

If you require help in the interpretation of this policy, contact the Data Protection Officer

Abbotskerswell Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

1. Introduction

1.1 This policy outlines the framework that governs how Abbotskerswell School and its staff must handle personal data to ensure compliance with the EU General Data Protection Regulation (GDPR) and associated data protection laws applicable in the UK.

2. Scope

2.1 This policy applies to the processing of personal data which is defined by article 4 of the GDPR, and to the processing of special categories of personal data defined by article 9 of the GDPR.

2.2 This policy and its supporting guidance shall apply to all Abbotskerswell School employees, agency and temporary staff, contractors, members and third-party staff, who have access to information systems or information used for School purposes.

2.3 Where this policy reads “staff”, it should be read to include all the entities in paragraph 2.2.

3. Legislation

3.1 Abbotskerswell School processes a variety of personal data to enable us to deliver a range of education services. Therefore, Abbotskerswell School is required to comply with the GDPR as well as other supporting legislation which governs the processing of personal data.

3.2 When handling and managing information the School and its staff shall comply with other legislation in addition to the GDPR, to include but not limited to:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
- Human Rights Act 1998
- Local Government Act 1972
- Local Government Act 2000
- Regulation of Investigatory Powers Act 2016
- Re-use of Public Sector Information Regulations 2005

4. Breach of this policy

4.1 All reckless or deliberate breaches of this policy will be investigated and may be referred to the Human Resources Department who will consider whether disciplinary action should be taken against the member of staff concerned. Alleged breaches of this policy will also be investigated by the Data Protection Officer as an information security incident in accordance with the Security Incident Management Policy and Procedure and may also be referred to

Human Resources and senior management as considered necessary.

5. Policy review

5.1 This policy will be reviewed by the Data Protection Officer on an annual basis. Formal requests for changes should be sent to the Data Protection Officer Jayne Edwards

6. Responsibilities

6.2 Responsibility for GDPR compliance rests with the Head Teacher. The Data Protection Policy and its supporting guides and standards are managed, maintained and communicated to staff by the Data Protection Officer.

6.3 The School's Information Asset Owners and Information Asset Administrators are responsible for ensuring that appropriate structures and procedures are in place to manage their information effectively. They are also responsible for ensuring that staff are made aware of, and comply with this policy, its associated standards and procedures. All staff are personally responsible for complying with this policy and supporting standards.

7. The data protection principles

7.1 The GDPR is underpinned by six common-sense principles which governs the way that Abbotskerswell School must process personal data. These principles are outlined in article 5 of the GDPR and are summarised below.

- *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').*
- *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*
- *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*
- *Personal data shall be 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 ('accuracy')*
- *Personal data shall be 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 shall be 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 ('integrity and confidentiality').*

7.2 Sections 8 - 20 outlines the steps that staff must follow when processing personal data to ensure compliance with each of the principles listed above.

8. Lawful processing of personal data

8.1 Abbotskerswell School and its staff must process personal data fairly and will not process personal data or special categories of personal data unless one or more of the lawful grounds listed on the Inside Devon website apply.

9. Privacy notices

9.1 When collecting personal data, Abbotskerswell School will make available the information contained in our template Privacy Notice. This may be available online and referenced on data capture forms, directly referenced on documentation or provided verbally. If Abbotskerswell School receives personal data from third parties, we will ensure that the information contained in a privacy notice, is made available to a data subject as soon as practical. This will usually be at the first point we are required to communicate with the data subject.

9.2 Further advice on Privacy Notices is available on the Inside Devon website. For more detailed assistance contact the Data Protection Officer.

10. Consent

10.1 Abbotskerswell School is only required to obtain someone's consent if there is no other legal basis for processing their personal data. If we are required to obtain consent, we will ensure that the following requirements are met;

- The consent is freely given
- The person giving consent understands fully, what they are consenting to
- There must be a positive indication of consent (opt-in as opposed to opt-out)
- The person giving consent must be able to withdraw their consent at any time
- Consent should be documented so that it may be referred to in the future, if necessary

10.2 Children under the age of 13 merit specific protection regarding their personal data. Such specific protection should apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data regarding children when using services offered directly to a child. If Abbotskerswell School is required to deliver such services to children, it will ensure that the requirements of article 8 of GDPR are met.

11. Rights of data subjects

11.1 Chapter 3 of the GDPR outlines the rights afforded individuals in respect of the processing of their personal data. These rights are summarised below;

- The right to transparency in respect of the processing of their personal data
- The right of subject access
- The right to rectification
- The right to erasure
- The right to restriction of processing
- The right to data portability
- The right to object to processing
- The right to request human intervention if processing is by automated means

11.2 Requests to exercise any of these rights are managed by the Data Protection Officer. The School's procedures for managing such requests are available and shall be adhered to

whenever Abbotskerswell School receives a request from someone wishing to exercise these rights.

11.3 When designing, implementing or procuring systems or services, Abbotskerswell School must ensure that those systems or services can allow members of the public to exercise any of the rights listed in section 11.1. Any systems or services found to be incapable of managing such requests, should be referred to the Data Protection Officer and must be subject to a privacy impact assessment.

12. Privacy by design

12.1 Article 29 of the GDPR creates a statutory obligation on Abbotskerswell School to ensure that a privacy impact assessment is undertaken on all new systems, processes or procedures that intend to process personal data, prior to their implementation. Such assessments are to be carried out by or in consultation with the Data Protection Officer. All assessments undertaken will be carried out in accordance with the School's Privacy Impact Assessment Procedure.

12.2 Compliance risks identified following a privacy impact assessment will be presented to relevant Information Asset Owners, Information Asset Administrators and or the Senior Information Risk Owner (SIRO) in accordance with the School's Information Assurance Policy.

12.3 If following the completion of a privacy impact assessment, Abbotskerswell School identifies processing activities assessed as high risk that cannot be mitigated to an acceptable level, the authority will consult with the Information Commissioner's Office prior to implementing the proposed processing activity, system or process.

13.0 GDPR and procurement

13.1 Abbotskerswell School is committed to upholding the confidentiality, availability and integrity of information that is processed by our contractors on our behalf. Underpinning this commitment, we will ensure that the following measures are followed when procuring goods and services that involve the processing of personal data.

- A privacy impact assessment is undertaken prior to any procurement which involves the processing of personal data
- A security questionnaire is completed to ascertain the technical and organisational measures that prospective contractors will put in place to protect the data that they will processing on behalf of Abbotskerswell School. The results of which will inform on the final decision as to whether the School contracts with that organisation.
- When procuring goods and services that requires a formal procurement exercise, we will ensure that contractual provision is in place which clearly identifies the following; who is the data controller; what data is being processed; a record of processing activity (in accordance with article 30 of the GDPR); arrangements for how personal data will be disposed of or returned to the School at the end of the contract; contractual clauses which mandate conformance to the GDPR.
- When procuring goods or services that do not require a formal procurement exercise, and which involve the processing of personal data, staff must ensure that they follow the School's Guide to security during procurement.

13.2 Where risks are identified during a formal or informal procurement process, these will be managed in accordance with the School's Information Assurance Policy.

14. Records of processing activity

14.1 Information Asset Owners will ensure that records of the processing activity are maintained for all information assets under their direct responsibility. Such records will include the information required in article 30 of the GDPR. Such records are to be made available to members of the public, the Information Commissioner's Office (or other supervisory authority as required) or the European Data Protection Board on request.

14.2 Abbotskerswell School will have measures in place to ensure that data processors responsible for processing personal data on behalf of the School, will maintain records of processing as required by article 30 of the GDPR.

15. Security incident management and notification

15.1 An information security incident can occur when the confidentiality, availability and or integrity of personal data is put at risk. Examples of activities considered an information security incident might include; information being at risk of or being lost; stolen; disclosed to the wrong recipients (accidentally or deliberately); accessed or attempted to be accessed unlawfully and/or without the permission of the School; sold or used without the permission of the School or a system containing personal data or sensitive business data malfunctions and the information is irretrievable indefinitely or for a long period of time.

15.2 Abbotskerswell School has a Security Incident Management Policy and Procedure in place which governs how the School and its staff must report and handle incidents. This policy and procedure must be followed at all times.

15.3 In accordance with article 33 of the GDPR, Abbotskerswell School is committed to notifying the Information Commissioner's Office or relevant supervisory authority within 72 hours, of being notified of an information security incident that might adversely affect the rights and freedoms of a data subject. Notifications of this nature are the responsibility of the Data Protection Officer, who will ensure that the risks associated with information security incidents are recorded, monitored and where appropriate escalated in accordance with the School's Information Assurance Policy.

16. The Data Protection Officer

16.1 Article 37 of the GDPR requires that Abbotskerswell School appoints a Data Protection Officer to undertake the tasks outlined in article 39 of the GDPR. Contact details for the Data Protection Officer will be made publicly available and will be referred to in all privacy notices.

16.2 Abbotskerswell School will commit to ensure that the Data Protection Officer is sufficiently resourced to undertake the tasks assigned to them under article 39 of the GDPR. The School

will also ensure that the Data Protection Officer is consulted on all matters which concern the processing of personal data.

16.3 The Data Protection Officer will act as the single point of contact for the Information Commissioner's Office or other relevant supervisory authorities and will ensure that compliance risks are reported to the highest level of management within Abbotskerswell School as required.

17. Transfers outside the European Economic Area

17.1 Abbotskerswell School will not transfer personal data to countries outside of the European Economic Area (EEA) unless one or more of the following qualifying criteria are met;

1) An adequacy decision has been made in accordance with article 45 of the GDPR
2) The transfer is the subject of appropriate safeguards in accordance with article 46 of GDPR
3) The transfer is the subject of binding corporate rules in accordance with article 47 of the GDPR
4) If one or more of the special circumstances outlined in article 49 of the GDPR are met

17.2 Any transfers of personal data to countries outside of the EEA will be subject of a privacy impact assessment prior to the transfer taking place. Decisions taken in respect of any transfers will be made in accordance with the School's Information Assurance Policy.

18. Information and cyber-security

18.1 The Data Protection Officer is responsible for the creation and communication of guidance on information security. This guidance will be routinely reviewed to ensure accuracy, with amended and new guidance communicated to staff on a regular basis.

18.2 Staff who are required to process personal data, in whatever format, must ensure that they follow the relevant guidance on information security. If it is found that this guidance has not been followed, this will be treated as an information security incident and will be investigated in accordance with the Security Incident Management Policy and Procedure. Where such actions are considered negligent, reckless or malicious, this will be referred to Human Resources for consideration as to the merits of disciplinary action.

18.3 Should it be considered necessary for staff to be excused from following the requirements outlined in any guidance on information security, these requests will be the subject of a privacy impact assessment.

19. Sharing personal information

19.1 Abbotskerswell School will only share personal data contained in its records with individuals who have a legitimate and legal right to view or receive it. Disclosures of personal data shall be proportionate and necessary and made in line with the School's policies and procedures. All disclosures shall comply with the GDPR and associated data protection

legislation, Human Rights Act 1998 and Common Law Duty of Confidence. More information about how and when to share information is available on the Knowing When to Share website.

20. Information assurance, compliance and reporting

20.1 Abbotskerswell School will have in place, an information assurance framework to aid in the identification, management and ownership of information risks. This framework is outlined in the School's Information Assurance Policy.

20.2 All information risks identified when working with services, following privacy impact assessments or from information security investigations, will be managed in accordance with the Information Assurance Policy. Compliance risks that are identified will be monitored by the Data Protection Officer and reported on a regular basis, to Information Asset Owners, Information Asset Administrators and to the Senior Information Risk Owner (SIRO).

21. Policy History

21.1 This Policy is maintained by the Data Protection Officer and will be reviewed on an annual basis. For help in interpreting this policy, contact Marie Farrelly.

Data Protection – Data Breach Policy

1. Introduction

Abbotskerswell School issues this policy to meet the requirements incumbent upon them under the Data Protection Act 2018 for the handling of personal data in its role as a data controller, such personal data is a valuable asset and needs to be suitably protected.

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidently) to avoid a data protection breach that could compromise security.

A data breach is defined as the compromise of information's confidentiality, integrity, or availability which may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2. Scope

This policy applies to all employees of Abbotskerswell School including contract, agency and temporary staff, volunteers and employees of partner organisations working for Abbotskerswell School.

3. Data Breaches

For the purposes of this policy data breaches will include both suspected and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*
- Equipment failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data *(e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)*
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- Breaches of policy such as
    - Server Room door left open
    - Filing cabinets left unlocked
    - Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

4. Reporting

The quick response to a suspected or actual data breach is key. All consumers in scope of this policy have a responsibility to report a suspected or actual data breach. If this is discovered or occurs out of hours

then this should be reported as soon as practically possible. This should be done through the completion of the reporting form in Appendix 1, which is sent to Marie Farrelly who will liaise with its Data Protection Officer (i-west).

5. Security Incident Management (SIM)

The organisation's lead officer shall complete the following phases of SIM (which are detailed in Appendix 2) with advice from its Data Protection Officer:

a) **Preparation** – the organisation will understand its environment and be able to access the necessary resources in times of incidents. It will also ensure its staff are aware of how to identify and report breaches

b) **Identification** – the organisation will determine whether there has been a breach, or a near miss, it will also assess the scope of the breach, and the sensitivity on a risk basis.

c) **Containment & Eradication** – the organisation will take immediate appropriate steps to minimise the effect of the breach. It will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause, and will establish who may need to be notified as part of the initial containment and will inform the police and other enforcement bodies where appropriate.

d) **Recovery** – the organisation will determine the suitable course of action to be taken to ensure a resolution to the incident. This may include re-establishing systems to normal operations, possibly via reinstall or restore from backup.

e) **Wrap Up / Learning from Experience (LfE)** – an assessment will be made on the likely distress on any affected data subjects. This will then form the decision on whether to report this to the regulator (ICO) which must be reported within 72 hours, and to the affected data subjects which must be done without undue delay. The organisation's Communications / Press Team may also be notified to handle any queries and release statements.

   A review of existing controls will be undertaken to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

   - Whether policy controls are sufficient
   - Whether training and awareness can be amended and/or improved
   - Where and how personal data is held and where and how it is stored
   - Where the biggest risks are apparent and any additional mitigations
   - Whether methods of transmission are secure
   - Whether any data sharing is necessary

   If necessary a report recommending any changes to systems, policies and procedures will be considered by the senior management board. This will include the decision on whether to report to the regulator and affected data subjects.

Phases (b) to (e) will form part of the investigation process. This process should commence immediately and wherever possible within 24 hours of the breach being discovered or reported.

6. Monitoring and compliance

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the senior management board.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

Appendix 1 – Data Incident Reporting Form

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date (and time where possible) of notification to the organisation	*If there was any delay in reporting the incident, please explain why this was*
Who notified us of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why?	*Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes.*
2. Recovery of the data	
What have you done to contain the incident?	*eg limiting the initial damage, notifying the police of theft, providing support to affected data subjects*
Please provide details of how you have recovered or attempted to recover the data, and when	*Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it*
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	
Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware / informed?	

Have any of the affected individuals made a complaint about the incident?	
Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?	
Your name and contact details:	

Appendix 2 - Security Incident Management (SIM): Record of work

This document provides the documented evidence and audit trail of a reported information security incident. It is designed to operate alongside the organisation's Data Protection Policy, and Data Breach Policy.

This form is to be completed by the Incident Handler(s) in the organisation.

The incident may require additional input and support from the organisation's Data Protection Officer, ICT, and potentially other specialist bodies (e.g. National Cyber Security Centre – NCSC)

Incident No:	
Severity (H, M, L):	
Basis for initial severity rating:	
Incident Handler(s):	
Date reported to organisation:	
By whom:	
Date reported to Incident handler:	
By whom:	
Date incident occurred:	
Senior Management notified (date):	

Summary of breach:	

Incident Response Phase	Evidence/Actions Taken
1. Preparation Gather and learn the necessary tools, become familiar with your environment	• Necessary staff trained on incident handling and incident response • Policy, Procedures & Guidance • Network Diagrams are held • The Record of Processing Activities (RoPA) will provide details of data, owners, custodians, and third parties – link to the RoPA • ICT also record event logs and hold logs on other systems (e.g. emails, firewalls etc) • Key contacts
2. Identification Detect the incident – Is it an incident (breach of policy), a near miss, or a data breach? Determine its scope, and involve the appropriate parties	
3. Containment Contain the incident to minimize its effect on other IT resources	
4. Eradication Eliminate the affected elements e.g. remove the malware and scan for	

anything remaining	
5. Recovery Restore the system to normal operations, possibly via reinstall or backup.	
6. Wrap Up Document the lessons learned and actions to reduce the risk of the incident/breach/near miss re-occurring Document the decision to report to both the affected data subjects and the ICO.	
	If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay **Decision to report to Data subjects** - Yes / No Based on: Officer: Signed: Date:
	Establish the likelihood and severity of the resulting risk to people's rights and freedoms - A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned **Decision to report to ICO** - Yes / No Based on: Officer: Signed: Date: