BROAD CHALKE CE VA PRIMARY SCHOOL
Data Protection Policy 2019

Mission Statement: With the love of God we learn, care, grow and share

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 General Data Protection Regulation (GDPR) which are part of the Data Protection Act 2018 (DPA 2018).. 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 GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual including: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (fingerprints, retina and iris patterns), where used for ID • 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 as a data controller with the ICO and will renew this registration annually or as otherwise 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. Our DPO is Mrs Michaela Johns and is contactable via the school office Tel: 01722 780212 or email admin@broadchalke.wilts.sch.uk

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

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 Headteacher or 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 European Economic Area
    - If there has been a data breach
    - Whenever they engage 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 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
- Be processed in a manner that ensures appropriate security of the personal data and is in accordance with the rights of the data subject
- Be kept securely
- Not be transferred outside the EEA (European Economic Area) unless the country offers adequate protection.

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 e.g. 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,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school 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 which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

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

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.

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 Information and Records Management Society's Retention Guidelines for Schools.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide 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 data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

- **Other schools**

If a pupil transfers from Broad Chalke CE Primary School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination authorities**

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Educational division**

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

- **Right to be Forgotten:**

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors. However, there are circumstances where the school has a legal duty to keep the information for a set retention period e.g. SEN, Child Protection.

9. Subject access requests and other rights of individuals

9.1 Subject access requests (See Appendix C)

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
- 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

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

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

If staff receive a subject access request 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 20 working days of the request
- 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 will not disclose information if it:

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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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.

11. CCTV (See also CCTV Policy)

We use CCTV around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and

accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the School Business Manager, Mrs Andi Chalke via the school office.

12. 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.

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 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.

13. 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 DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- 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
- 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data Disposal

- The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.
- Broad Chalke School will dispose of paper copies of personal data securely at the end of each academic year unless we have a specified retention period in Appendix A. Whoever is the Headteacher at the end of the retention period will be responsible for ensuring the secure destruction of the data.
- The school has identified a qualified source for disposal of IT assets and collections.

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 E.

When appropriate, we will report the data breach to the ICO within 72 hours. 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 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. Auditing

The school must be aware of **all** the personal data it holds, be it electronic or paper.

- A register (Appendix A) will be kept detailing the types of personal data held, where and by whom, and will be added to as and when new data is generated.
- How long these documents need to be kept will be assessed using the Records Management Toolkit or by a decision taken by the Headteacher (HT)
- Audits will take place in line with the timetable. (Appendix B).
- Appendix D details the Staff Computer Policy

18. Privacy Impact assessments (PIA)

The school will carry out a risk assessment to establish what security measures are already in place and whether or not they are the most appropriate and cost effective available. The aim of a PIA will always be a minimisation of privacy risk and will generally involve assessing:

- How sensitive is the data?
- What is the likelihood of it falling into the wrong hands?
- What would be the impact of the above?
- Does anything further need to be done to reduce the likelihood?

Risk assessment will be an on-going process and the school will have to carry out assessments at regular intervals as risks change over time.

19. Securing and handling data held by the school

The members of staff responsible for data protection are mainly Amanda Brockway (Head Teacher) and Andrea Chalk (School Business Manager). However all staff must treat all pupil information in a confidential manner and follow the guidelines as set out in this document to 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. The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secure when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access at the end of the school day
- Staff and pupils are reminded to change their passwords at regular intervals
- The school will keep and delete necessary pupil and staff information in accordance with the Records Management Society's guidance.
- The school is also committed to ensuring that staff are aware of data protection policies, legal requirements and adequate training is provided to them.
- Hard copy data, records, and personal information are stored out of sight and in locked locations. The only exception to this is medical information that may require immediate access during the school day.
- Unwanted paper copies of data, sensitive information or pupil files will be shredded. This also applies to handwritten notes if the notes reference any person by name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, laptop or mobile device, staff must ensure that the documents are properly shut down before leaving the computer unattended.
- All staff should operate a CLEAR DESK policy to avoid personal data being seen by unauthorised people.
- Personal data should not be transmitted in unsecured emails (e.g. pupil names and addresses, performance reviews etc.).
- Data transfer should be through secured websites e.g. S2S, Perspective Lite, common transfer files and school census data. If this is not available then the file must be minimally password protected before sending via email, the password must be sent by other means preferably by telephone and on no account included in the same email.
- Data (pupil records, SEN data, contact details, assessment information) will be stored in a secure place – e.g. locked filing cabinet / password protected laptop/ password protected server/remote backup.
- When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by a technician using a recognised tool.
- The school will ensure that staff that are responsible for information, such as SEN, medical etc. know what data is held, who has access to it, how it is retained and disposed of.
- Where a member of the school has access to data remotely (e.g. SIMS from home), remote access off the school site to any personal data should be over an encrypted connection (e.g. VPN) protected by a username/ID and password. This information must not be stored on a personal (home) computer, laptop or mobile device.
- Members of staff (e.g. senior administrators) who are given full, unrestricted access to an organisation's management information system should do so over an encrypted connection and use two-factor authentication, which is available to SIMS users from Capita. This information must not be stored on a personal (home) computer, laptop or mobile device.
- Where personal information needs to be taken off site, staff must inform the Headteacher
- The school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils. In these situations the data must be kept confidential, transported securely and stored in a secure location.
- If an encrypted USB stick is used, the data should not be transferred from this stick onto any home or public computers.
- Paper copies of data or personal information should only be taken off the school site if necessary to fulfil professional duties but this should be avoided where possible. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- 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.

20. Fair Processing / Privacy Notice

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of an individual's data.

The Governing body and DPO are responsible for monitoring and reviewing this policy.

Links with other policies

This data protection policy is linked to our: Freedom of information publication scheme; Online Safety and Acceptable Use Policy; Child Protection Policy; CCTV Policy.

Ratified by FGB: Spring 2013
Reviewed: Spring 2015, Spring 2017, Spring 2018, Spring 2019
Next Review due: Spring 2020

Appendix A: Register of <u>personal data</u> held by the school

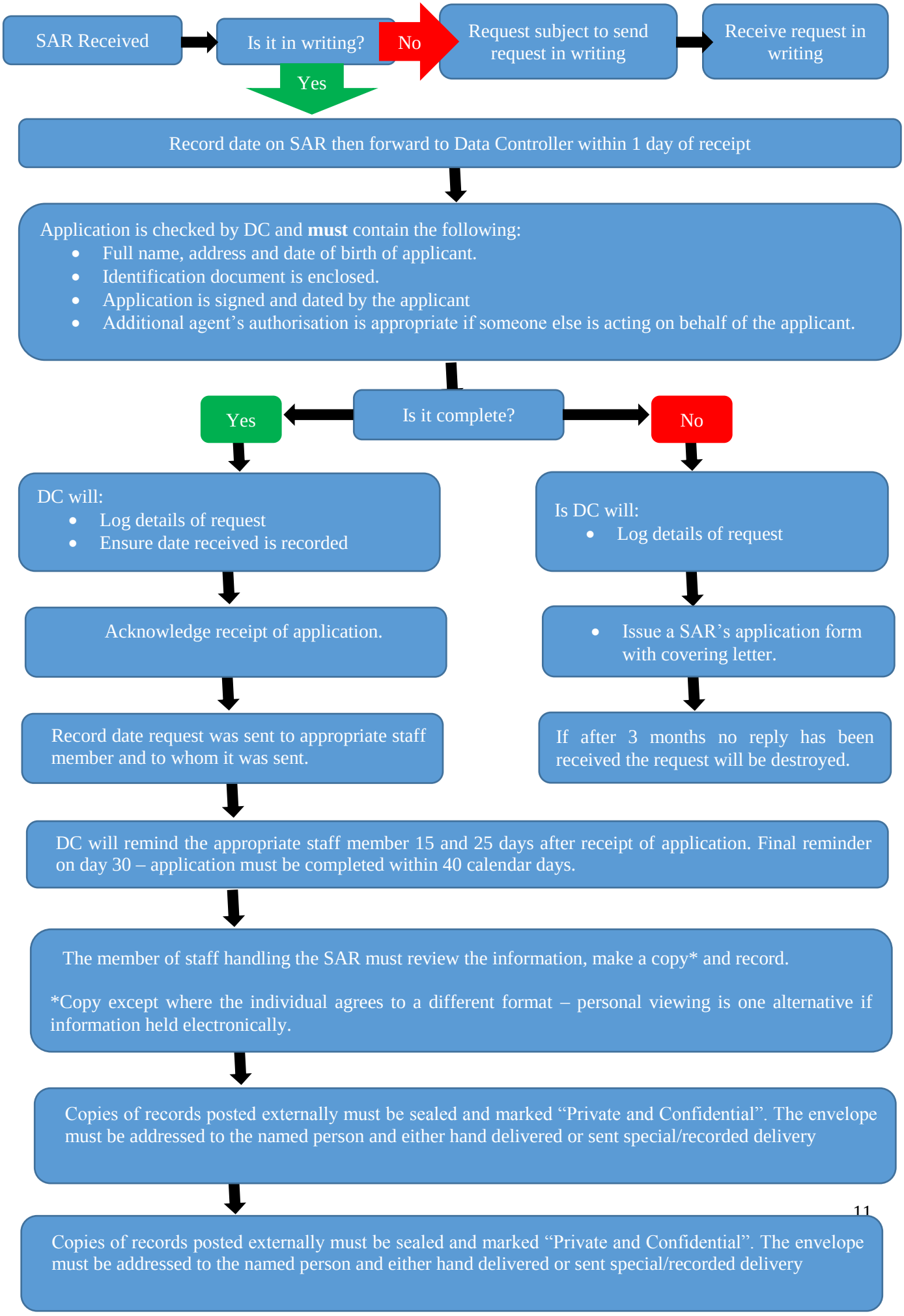
Type of data	Held on	Period to be retained	Type of protection	Who can access the data
Child Protection File	File in locked cabinet in office	DoB + 25 years	Password protected laptop. Locked cabinet	HT
Pupil SEN data	Curriculum and Admin servers. Paper copies for teachers in class SEN folders which move up with the child.	1 main copy Closure + 25 years	Password on Servers, laptops and office PC Paper copies of Support Plans are NOT to be taken off school site. SEN Paper Register kept in secure location	SENCO, admin, TAs, Teachers and HT
Attendance data	Admin server	Until pupil is 18	Password on Servers, laptops and office PC	HT, admin.
Personal information and characteristics e.g. ethnicity	Admin server	Until pupil is 18	Password on Servers, laptops and office PC	HT, admin.
Racist incident log	File in locked cabinet in office	Until pupil is 18	Initials but no names Access to school office is limited to staff	Admin and HT
Pupil FSM data	Curriculum and Admin servers.	Until pupil is 18	Password on Servers, laptops and office. Paper Records kept in secure location	HT, staff, admin.
Pupil reports	Curriculum and Admin servers. Staff laptops, temporarily on USB sticks then wiped	Until pupil is 18	Password on Servers, laptops and office PC	SENCO, Admin , Teachers and HT
Whole school data through ASP / FFT/ Perspective Lite	Web based and paper	Until pupil is 18	Password on Servers, laptops and office PC Paper Records kept in secure location	Password issued by Admin or HT
Serious behaviour incidents	curriculum server	Until pupil is 18	Password	Admin, Teachers and HT
EYFS data	Curriculum and Admin servers. Paper for EYFS teacher / HT	Current year + 6 years	Password on Servers, laptops and office PC EYFS Paper Records kept in secure location	HT, EYFS staff, admin
KS1 / KS2 SATS	Curriculum and Admin servers. Paper copies for teachers and HT	Current year + 6 years	Password on Servers, laptops and office PC SATS Paper Record kept in secure location	HT, staff, admin
Classroom Monitor – attainment and progress	Curriculum and Admin servers. Paper copies for teachers and HT	Current year + 6 years	Password on Servers, laptops and office PC Paper Records kept in secure location	HT and teachers
Information relating to staff e.g. Performance Management reviews, references	Curriculum and Admin servers. Paper copies for teachers and HT	Current year + 6 years	Password on Server and laptops Password protected file Paper Records kept in secure location	HT and Deputy Head
Letters to parents of a sensitive nature	Heads laptop	While pupil is at school + 3 years	Password on Servers, laptops and office PC	HT

Medical information	Locked cabinet Emergency medical info displayed in kitchen, staffroom and office with permission.	While pupil is at school + 3 years	Password on Servers, laptops and office PC Door to First Aid room shut but not locked	All staff
Photographs	Admin server curriculum server	While pupil is at school + 3 years (unless historical record e.g. class/ whole school / team photos)	Password on Servers, laptops and office PC	Admin, Teachers and HT
Minor behaviour incidents	curriculum server	While pupil is at school + 3 years	Password	Admin, Teachers and HT
Registers of pecuniary interests	File in locked cabinet in First Aid Room	Current year + 3 years	Locked cabinet	Admin and HT
Contact details	Office PC and File in office with paper contact details	Just while pupil is at school	Password Access to school office is limited to staff	Electronic – office staff only. All staff have access to paper contact details
Dates of birth and addresses	Office PC and in office File in locked cabinet in office	Just while pupil is at school	Access to school office is limited to staff	Electronic – office staff only. Staff have access to paper contact details
Governor minutes and reports	Sent by email to personal governor email addresses. All pupil and staff data is anon.	For term as governor	Governors to return folders of minutes to school at the end of their term as governor.	Only the governor
Staff Email	RM Unify	3 years	Password on Servers, laptops and office PC	All school staff with access to school email
Class based assessments e.g. mark books	Curriculum server. Heads and teachers laptops	Current year + 1 year	Password on Servers, laptops and office PC Paper Records kept in teachers desks	Teachers and HT
Staff meeting minutes	Staff files	Current year + 1 year	Record so that there is no personal data.	All staff
Single Central Record	On Office PC and in locked cabinet	Updated at least annually	Password protected Locked cabinet	Admin and HT

Appendix B: Timetable for Information Security Management

Activity	**Frequency**	**Lead**
Audit of data held	Annually	Head and SBM
Encrypting personal data	On-going	All staff
Reviewing data backup procedures	Annual	SBM
Wiping of laptop data when re-issued	As necessary	ICT Technician
Wiping of laptop data when discarded	As necessary	ICT Technician

Appendix C Subject Access Request Flowchart



Appendix D

BROAD CHALKE CE VA PRIMARY SCHOOL

Staff Computer Use Policy (includes PC, Laptop and mobile devices)

Mission Statement: With the love of God we learn, care, grow and share

- Passwords that I use to access school systems will be kept secure and secret – if I have reason to believe that my password is no longer secure I will change it. Passwords to access school systems will routinely be changed every 6 months.
- I acknowledge that the computer provided for me to use remains the property of the school and should be used for school business.
- I will not alter the files of others held on the server.
- I will not update web content or use pictures or text that can identify the school, without the permission of the HT.
- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school. I will seek permission with the school's technician / Network Manager should I need to install additional software.
- I will always adhere to the copyright.
- I will always log off the system when I have finished working particularly if working in an area accessible to pupils.
- I understand that the school may, in line with South West Grid for Learning, monitor the Internet sites I visit.
- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the school technician / Headteacher.
- Any e-mail messages I send will not damage the reputation of the school.
- All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be forwarded.
- I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.
- I understand that I am responsible for the safety of school data that I use or access.
- In order to maintain the security of data I will take the following steps:
    - ✓ I will store data files in my user area only for as long as is necessary for me to carry out my professional duties.
    - ✓ I will not save data files to a PC or laptop other than that provided by the school.
    - ✓ If I need to transfer personal data files and no secure electronic option is available I will only do so using the encrypted USB key provided by the school.
    - ✓ Personal data will only be sent electronically through a secure method, e.g. Perspective Lite. If this is not available then the minimum requirement is to password protect the document before attaching it to email.

If I am in any doubt as to the sensitivity of data I am using, I will consider these questions:

- Would disclosure / loss place anyone at risk?
- Would disclosure / loss cause embarrassment to an individual or the school?
- Would disclosure / loss have legal or financial implications?

If the answer to any of these questions is yes, then the data should be treated as sensitive.

I understand that if I do not adhere to these rules outlined in this policy, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow including notification to professional bodies where a professional is required to register. If an incident is considered to be an offence under the Computer Misuse Act or the General Data Protection Regulations this may be reference for investigation by the Police and could be recorded on any future Disclosure and Barring Service (formerly known as Criminal Record Bureau) checks.

Appendix E: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the HT
- The HT will investigate the report, and determine whether a breach has occurred. To decide, the HT 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
- The HT will record this in the breach register.
- The HT will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The HT will inform the DPO if it is a serious breach
- The DPO will also assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will assess whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the breach register.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. 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. 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO

    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The HT will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The HT 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)
- The DPO and HT will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches
We will take the actions set out below to mitigate the impact of different types of data breach, 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 HT as soon as they become aware of the error
- In any cases where the recall is unsuccessful, the HT will 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 HT will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

Other types of breach could include:
- Non-anonymised pupil premium interventions being published on the school website
- Non-anonymised pupil results being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked