# Data Protection and Secure Data Handling Policy

| | |
|---|---|
| Review date | January 2023 |
| Date of next policy review | November 2023 |

*This policy is in line with the Single Equality Policy*

**Princecroft Primary School**
**Princecroft Lane**
**Warminster**
**Wiltshire**
**BA12 8NT**

**Headteacher: Mrs Gemma Pierson**

**E-mail: admin@princecroft.wilts.sch.uk**

**This policy has been guided by, and is in accordance with the provisions of, the following documents:**

- The Data Protection Act 2018, The Data Protection, Privacy and Electronic Communications (Amendments) (EU Exit) Regulations 2020
- Data Protection: toolkit for schools (DfE August 2018): https://www.gov.uk/government/publications/data-protection-toolkit-for-schools
- Data protection for Education Providers (31/12/20)
- Information and Records Management Society: Information Sharing - Advice for practitioners providing safeguarding services to children, young people, parents and carers (DfE July 2018)
- Freedom of Information Toolkit and Procedures

**Also relevant in this area are the Princecroft policies on:**

- Safeguarding and Child Protection, Online Safety and the Code of Conduct for Staff

**CONTENTS:**

4. Data Rectification Request Form
5. Data Deletion Request Form

## 1. General Principles:

- We recognise that schools have increasing access to a wide range of personal data, commercially sensitive financial data and sensitive information about pupils, parents and staff, some of which we are legally required to gather and process in order to carry out our duties as a public authority, but also to support the development of pupils (educationally, socially and emotionally), to protect the pupils in our care and to facilitate the efficient running of the school.
- Data and records provide evidence for protecting the legal rights and interests of the school and provide evidence for demonstrating performance and accountability.
- Under the UK Data Protection Legislation (as listed above) there are strict legal guidelines in place as to how data should be both 'controlled' and 'processed', which the school is fully aware of and complies with.
- The amount of data held by the school will be reduced to the minimum necessary to fulfil its statutory obligations and legitimate school and pupil management needs.
- Data held by the school will be routinely assessed to consider whether it needs to be retained.
- Personal data held by the school will be safely and securely stored (electronic or hard copy) and sent by secure means.
- These regulations apply to 'personal data', 'special categories of personal data' and personal data relating to 'criminal convictions and offences'.
- This policy applies to all data and records created, received or maintained by school staff in the course of carrying out its functions. It is the responsibility of all members of the school to take care when handling, using or transferring personal data to ensure that it cannot be accessed by anyone who does not have permission to or a need to access that data.

## 2. Key Definitions:

- **Commonly used data format** means the format in which the data is stored must be widely used and well-established.
- **Data controllers** determine the purposes and means of processing personal data.
- **Data processors** are responsible for processing personal data on behalf of a controller.
- **Data protection impact assessments** are required when introducing new technology for the handling and processing of personal data and when data is processed on a large scale. They assess the level of risk involved and the security measures that need to be put in place to protect individuals.
- **Information Commissioners Office (ICO)** is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
- **Personal data** is defined as any information relating to an identifiable person who can be directly or indirectly identified, including by reference to a unique indicator such as a 'unique pupil number (UPN)'.
- **Personal data breaches** are defined as a security incident that has affected the confidentiality, integrity or availability of personal data. A personal data breach takes place whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation or if the data is made unavailable and this unavailability has a significant negative effect on individuals.
- **Records** are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its
-

transactions or activities. These records may be created or maintained in hard copy and/or electronically.

- **Special categories of personal data** (previously referred to as 'sensitive data'), demanding a higher level of protection specifically refers to information held and processed about an individual relating to:
  - racial or ethnic origin
  - political opinions
  - religious or other philosophical beliefs
  - trade union membership
  - genetic or biometric data
  - physical or mental health
  - sexual orientation
  - criminal convictions or offences

  and, as this data, by its very nature could create more significant risks to a person's fundamental rights and freedoms, there are additional safeguards in place. Processing of these special categories is prohibited, except in limited circumstances set out in Article 9 of the UK GDPR.
- **Structured Data** is data which can be extracted by software (e.g. from a spreadsheet) as is therefore normally machine readable.
- **Subject Access Requests** gives individuals the right to see a copy of the information an organisation holds about them.
- **Third countries** is any country outside the United Kingdom
- **Unstructured data** is the **collective name for the information that your organisation creates, and keeps**, to help it carry out its primary tasks, but isn't in a recognisable structure or contained in a database

## 3. Requirements of the UK General Data Protection Regulations (UKGDPR)

- Under the UK GDPR (Article 6 of the 'Keeling Schedule') the data protection principles set out the main responsibilities for organisations which require that personal data shall be[1]:
  - **a)** processed lawfully, fairly and in a transparent manner in relation to the data subject (lawful, fairness and transparency)
  - **b)** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
  - **c)** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
  - **d)** accurate and, where necessary, kept up to date with every reasonable step being taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
  - **e)** kept in a form which permits identification of the data subjects for no longer than is necessary for the personal data to be processed, and
  - **f)** processed in a manner that ensures appropriate security for the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures

[1] See Article 6 of the General Data Protection Act for full legal terminology

## 4. Responsibilities:

**The School:**

- has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment and the person with overall responsibility for this policy is the Head Teacher (for more detail see sections below on '**Documentation**' and '**Accountability and Governance').**
- is required to appoint a Data Protection Officer (DPO) to oversee the collection, processing and security of data and the person responsible at Princecroft is based at **One West** and can be contacted through the school office.
- as both a controller and processor of personal data, has a responsibility to register with the 'Information Commissioner's Office' and to renew the registration annually.
- must inform pupils, parents, staff and governors (through the issuing of **Privacy Notices** – see section below) what data they are required to collect and retain and the lawful basis for processing personal data as defined by Article 6 of the UK GDPR.
- must, through the same Privacy Notices also inform pupils, parents, staff, and governors of any special category data and/or data on criminal convictions or offences, they hold, together with the lawful basis for that processing as defined in Articles 6 and 9 of the 'Keeling Schedule'.
- follows the guidance with regard to information sharing of data related to safeguarding and child protection as set out by the Department of Education (DfE)
  Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (DfE July 2018).
- must produce and maintain, through an annual audit an 'Information Asset Register' detailing all data that it holds (see section 7 below). This register must be kept, detailing the types of sensitive data held, where held and by whom it is accessed. A copy of this register can be found on our school website.

**Sharing and/or receiving personal data between the UK and third countries**

- Where we need to transfer personal data which is either undergoing processing or is intended for processing in a third country or to an international organisation we will follow the procedures as outlined in Chapter 5 (Articles 44 and 45 of the 'Keeling Schedule').
- We have identified what data, if any, we receive from third countries and are aware who the data controller and processors of that data are and where the data is stored.
- We understand that we are responsible for carry out our own risk assessment and that we are complying effectively with UKGDPR.

**The Data Protection Officer (DPO):**

- informs and advises the school and its employees about their legal obligations to comply with the UK GDPR and other data protection laws.
- manages internal data protection activities and oversees regular data audits.
- is responsible for ensuring that the Information Asset Register is kept up to date and that staff are involved in an annual audit of its contents in relation to the files that they hold, and is the first point of contact for external supervisory authorities as well as those individuals (pupils, staff, parents and governors) whose data the school holds.
- advises on Data Protection Impact Assessments (DPIA)and ensures that they are carried out in advance of any processing of data likely to result in a high risk and that the impact on any of an individuals' rights and freedoms, including (but not limited to) privacy rights have been considered.
- ensures that when a DPIA concludes that there is a high risk, which cannot immediately be mitigated against, the ICO is consulted **before** any such data is processed.

- carries out regular risk assessments to ensure the most appropriate security measures are in place for information management.
- Coordinate and oversee the following data management activities and controls:

| Activity | Frequency | Lead |
|---|---|---|
| Maintenance of Info Management and Data Register | On-going | Finance and HR Assistant |
| Audit of data held and destruction of out-of-date records and data[2]. | Annual | Head and the Finance and HR Assistant |
| Encrypting sensitive data | On-going | All Staff |
| Reviewing data backup procedures | Annual | Finance and HR Assistant, IT Support Technician |
| Identifying staff responsible for data security and maintaining a log of names / roles | Annual | Head |
| Wiping of laptop data when re-issued and/or before disposal | As necessary | ICT Support |

**Individual Staff and Employees:**
- must ensure that records for which they are responsible are accurate, are stored securely and, are disposed of in accordance with the school's policies and records management guidelines.
- must ensure that when confidential data needs to be sent to another individual or organisation (whether that be in electronic format, hard copy or both) they follow the procedures as outlined in section 10 below.
- must contribute to the annual review of the Information Asset Register by advising the DPO of any additions or deletions from the register of records that they hold.

This will form part of staff induction and training procedures.

**Parents/Carers** (in respect of both themselves and their children)**, and Staff:**
- should ensure that the information they provide the school with is accurate and kept up to date.

## 5. Rights of Individuals on Whom Data is Held /Subject Access Requests

- The UK GDPR identifies 7 'rights' of individuals on whom data is held, some of which apply to schools and others which are aimed at commercial practices. Below is a summary of the guidance regarding each of these rights, but more detailed information can be found on the ICO website or by clicking on the links below. Hard copies of these documents can also be requested from the school office. There are 7 rights in relation to their personal data, as outlined by the UK GDPR are:
  - right to be informed (privacy notices)
  - right of access (subject access request)
  - right to rectification (correcting inaccuracies)
  - right to erasure (deletion of data when there is no compelling reason to keep it)
  - right to restrict processing (blocking or suppression of processing)
  - right to data portability

[2] The DofE provide guidance on the management of data records and a checklist for its annual review and safe destruction in its publication "Annual Review of School Records and Safe Destruction Checklist"

- right to object to the inclusion of information (based on grounds pertaining to their situation)

- Some of these rights may not apply, depending on the legal bases on which we hold and process the data but those rights, which are relevant to the class of person on whom data is held (parent/carers, pupils, staff, governors), are reflected in the respective data privacy notices at Appendices 1 to 5.
- An individual can make a request regarding any of the areas detailed below either verbally or in writing and they need not be directed towards a specific person or contact point. Requests can also be made by social media. However, we would encourage any individual wishing to exercise their rights to put their request in writing (see Appendix 2) and/or speak directly to the DPO or a member of the school's senior management team. A third party can also make a SAR on behalf of another person as long as the School has received confirmation that the third party has their permission.
- We have timescales in place to provide individuals with a response to any request they make but there may be exceptional circumstances (e.g. school closures) where it is not always possible to adhere to these time schedules. Where this is the case, individuals will be kept informed.
- In all cases we will justify our decision in writing and a copy will be kept on the school's files.
- Much of the data that schools are required to collect and process falls under our duty as a public authority in order for us to fulfil our legal obligations, and this basis is referred to as our 'public task'. In addition, we also hold data on other bases (as outlined in our Privacy Notices) namely, 'contract' (in relation to the staff we employ) 'consent' 'legitimate interests', 'legal obligation' and 'vital interests'.

**Right to be Informed**: **(Please also refer to the section below on 'Privacy Notices'**)

- At the time of requesting data from individuals (pupils, parents, staff, governors), the individuals must be informed of their rights regarding that data. You have the right to be told how the school processes your data and the reasons for the processing. In order to provide this information to you, Princecroft School has a privacy notice to explain what data we collect about you, how we collect and process it, what we process it for and the lawful basis which permits us to process it. Our privacy notices are published on our website.
- In the event that it becomes necessary for us to process personal data in a way that has not be detailed in the privacy notice already received, we will ensure that we bring this change to the attention of all individuals involved before we start processing.
- Where we have obtained personal data from another source (e.g. outside agency or another school) we will provide the individuals concerned with the necessary privacy information within a reasonable period of obtaining the data and no later than one month from receiving it.
- In addition, there may be times during the school year when we may require further information from you for a specific purpose. At that time, will advise you of any additional information regarding your rights as we are required by the UK GDPR.
- If we are reliant on 'consent' as our lawful basis, you will be ad vised of that and you will be required to give your consent in writing.

**Right of Access:**

- All individuals have the right to access their personal data and supplementary information and this is referred to as a 'Subject Access Requests (SAR)'. Appendix 2 gives more information on SARs in the form of 'Frequently Asked Questions'.
- The right of access allows individuals to be aware of and verify the lawfulness of the processing of their data. This right of access can also be exercised by a child, even if they are under the age of 16. However before responding to any such request, we retain the right to consider whether

or not the child is mature enough to understand their rights. More detailed information can be found in section 6 below.

- The information that we provide in response to any request will be in a concise, transparent, clear and easily accessible format. This will be particularly important where the information is addressed to a child.
- Individuals have the right to be provided with a copy of the information that is held on them free of any charge unless the request is manifestly unfounded, excessive[3] or repetitive, in which case the school reserves the right to charge a reasonable fee, based on the administrative costs of providing that information. Should this be the case, individuals will be advised of any charges in advance but we are not required to comply with the request until the fee has been received.
- A reasonable fee may also be charged for further copies of the same information.
- Information must be provided without delay and at the latest within one month of receipt of the request, or longer depending on when the request is made (see final bullet point).
- Where a request is complex or numerous, the school can extend the compliance period for a further two months as long as the individual requesting the information is informed that this will be the case within one month of the receipt of the request. The school will, at the same time, explain why this extension in time is necessary.
- Whilst it is always our aim to respond in a timely manner, given the nature of the school's academic year, should a request be received less than one month before the end of any term or within a school holiday period, the school will require an extended period of time in which to comply and this will be explained to the applicant at that time.
- The school reserves the right to refuse to respond to a request when they are manifestly unfounded or excessive, especially if they are repetitive. In such cases, the individual making the request will be informed of the school's decision not to comply together with the reason why, as well as informing them of their right to complain to the supervisory authority without delay and at the latest within one month.
- Where the request is made electronically, the school will provide the information requested in a commonly used electronic format unless you request us to supply it in another format.
- Where we hold a large amount of personal data about an individual, we can ask that the request be specific.
- If by responding to a SAR we would also have to disclose information about another individual who could be identified from the information supplied, we do not have to comply with the request unless the other individual has given their consent or it is reasonable for the school to proceed without their consent.

**Right to Rectification:**

- One of the fundamental principles underpinning data protection is that the data the school processes about you will be accurate and up to date. You have the right to have your data corrected if it is inaccurate or incomplete.
  If you wish to have your data rectified, you should do so by completing the data rectification request form in Appendix 4
- Where the school has disclosed this information to a third party (e.g. Department for Education or Local Authority) it is responsible for ensuring that the third party also corrects the data in question. The individual will be advised of any third parties to whom the data has been supplied, where appropriate.
- The school must ensure that data is rectified within one month but we may extend this period for a further two months where the request is complex.
- Where the school decides not to take action to rectify data at the request of an individual, we will explain why and inform them of their right to complain to the Information Commissioner.

[3] As defined in the ICO guidelines in each section on 'rights'.

- Where we feel that a request is manifestly unfounded or excessive, we can also refuse to comply with the request whilst explaining our reasons in writing to the individual concerned.
- Individuals may request a restriction of the processing of their data where they are contesting its accuracy and the school are checking it and, as a matter of good practice this request should be complied with even if the individual has not exercised their right to restriction (as detailed below).

**Right to Erasure**:

- Individuals have the right to request that their information is erased/deleted where there is no compelling reason for its continued processing i.e.:
  - where it is no longer necessary for the school to hold that data (bearing in mind the requirement to retain certain documents for a specific period of time)
  - when, if the data is obtained under the basis of 'consent' that consent is subsequently withdrawn
  - where data has been unlawfully processed or where an individual objects to the processing and there is no overriding legitimate interest for the processing to continue
- This right to erasure does not apply when:
  - we require the data to fulfil our legal obligations
  - for the performance of a task carried out in the public interest or in the exercise of official authority
  - for archiving purposes in the public interest, scientific research, historical research or statistical purposes where its erasure will impair those processes, and
  - for the establishment, exercise or defence of legal claims

If you wish to have your data deleted, you should do so by completing the data deletion request form in Appendix 5.

- The school has one month to respond to a request.
- The school can also refuse to delete the data if it has been processed for reasons such as defence of legal claims, public health or public interest.
  Refer to the ICO ***'When can the organisation say no?'*** for explicit details https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/
- In most cases we cannot charge a fee to comply with a request for erasure but we can charge a 'reasonable fee' for the administrative costs of complying with a request we believe to be manifestly unfounded or excessive, in the event that we agree to respond to that request. In such circumstances, we will not proceed until the fee has been received.

**Right to Restrict Processing:**

- In certain circumstances, individuals have the right to request the restriction or suppression of their personal data, which means that they can limit the way in which any organisation uses their data (as opposed to asking for their data to be erased). This right applies when:
  - an individual contests the accuracy of the data being processed and you are verifying the accuracy of that data
  - an individual believes that data has been unlawfully processed but opposes erasure and requests to restrict instead
  - the school no longer needs to keep the data but has been asked to do so in order to establish, exercise or defend a legal claim
  - an individual objects to the processing of the data and the school is considering whether its legitimate grounds override those of the individual in question
- Where the school has disclosed this information to a third party (e.g. Department for Education or Local Authority) it is responsible for ensuring that the third party also restricts the processing of the data in question, albeit temporarily. The individual will be advised of any third parties to whom the data has been supplied, where appropriate.

- The school can refuse to comply with a request for restriction if we believe the request to be manifestly unfounded or excessive (taking into account whether it is repetitive in nature) and we may either refuse to deal with the request or reserve the right to charge a fee in order to deal with it.
- We will justify our decision for any action we take in writing. In the event that we do refuse to comply or wish to charge a fee, individuals will be informed within one month of the receipt of the request (with exceptions being made for school holidays) and will advise individuals of our reasons, their rights to make a complaint to the ICO and their rights to seek a judicial remedy.
- Should the school decide it is appropriate to charge a fee or believe that we require additional information to identify an individual, no further action will be taken before that fee is received, after which the school still has one month to respond.

**Right to Data Portability**:

- The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller. The right to data portability only applies when:
  - the lawful basis for processing this information is consent **or** for the performance of a contract; and
  - the school is carrying out the processing by automated means (ie excluding paper files)

**Right to object**:

- Where applicable, individuals have the right to object on "grounds relating to their particular situation".
- Where an individual exercises their right to object, we are required to stop processing the personal data we hold unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.
- When an individual objects to the processing of data based upon a public task (including scientific or historical research) or legitimate interest they must give specific reasons why they are objecting to the processing of the data and these reasons should be based upon their particular situation.
- The school can refuse to comply if:
  - we can demonstrate compelling legitimate grounds for the process, which override the interest, rights and freedoms of the individual or,
  - the processing is for the established, exercise or defence of legal claims.
- Individuals are advised on their right to object in our Privacy Notice.
- The school has one calendar month to respond to an objection.

## 6. UK GDPR and Children

- Children need particular protection when collecting and processing their personal data as they may be less aware of the risks involved, particularly when you are relying on 'consent' as the lawful basis, especially for any online service. In such cases, only a child over the age of 13 can give consent.
- In the majority of cases, the data we collect on children does not rely on consent as the lawful basis but we need to ensure that in any correspondence with children, the language we use is clear and unambiguous.
- For children under the age of 13, we are required to get consent from whomever holds parental responsibility (unless the online service offered is a preventative or counselling service).

- Children have the same rights as adults over their personal data, including all the rights outlined above. Where a child is not considered to be competent, an adult with parental rights may usually exercise the child's data protection rights on their behalf.

**7. Privacy Notices:**

- The school will issue Privacy Notices in compliance with the requirements of the GDPR to all individuals on whom we hold data, at the time that they join our school, namely:
  - pupils (via their parents),
  - parents/carers
  - staff
  - governors
- Each type of Privacy Notices will contain the following information:
  - the categories of data that we hold
  - why we collect it
  - the lawful basis on which we process that data
  - who we share the data with
  - how long we retain the data
  - your right to access your data and your right to object
- The Privacy Notices for Staff and Governors are available in the School Office
- The Privacy Notices for Pupils and for Parents/Carers are published on the school website.

**8. Documentation**

- The UK GDPR contains explicit provisions regarding what we are required to document regarding the data we control. Article 30 states that we must document the following information (available both in electronic form on our website and as a paper copy), which can be obtained by request from the school office:
  - the name and contact details of our organisation
  - the contact details for our Data Protection Officer
  - the purpose of our processing
  - descriptions of the categories of individuals and categories of personal data who receives the personal data we process
  - our retention schedules (based on DfE guidance)
  - a description of our technical and organisational security measures
- Our Information Asset Register records the following information:
  - descriptions of the data that we hold (personal data, special category data and data relating to criminal convictions and offences)
  - the lawful basis for our processing with reference to Articles 6, 9 and 10 of the UK GDPR
  - in what format and how that data is held
  - how long we retain the data
  - how it should be disposed of/shredded

**9. Accountability and Governance**

Under the UK GDPR, the school is required to demonstrate that we comply with the principles of the accountability and responsibility and in order to do this we must:

- ensure that we implement appropriate technical and organisation measures which will include:
  - publication of this policy
  - on-going training for staff and relevant induction for new staff
  - internal audits of our processing activities, including data protection impact assessments for personal and/or special category data that is processed on a large scale

- internal audits of all the personal data we hold, including special categories of personal data which include the form that the data is held in, where it is held, who has access to it, the security measures in place and how long it is retained
- ensure that records are kept securely, in line with our legal obligations
- ensure that records are disposed of securely in line with our legal obligation.
- ensure that our records are kept up to date and reflect our current position, and
- in the unlikely event of a data breach, we will ensure that records are kept regarding the breach and the action we took in response to it

## 10. Personal Data Breaches

- Personal data breaches can include:
  - access to the data we hold by an unauthorised third party
  - deliberate or accidental action (or inaction) by a controller or processor
  - sending personal data to an incorrect recipient
  - computing devices containing personal data being lost or stolen
  - alteration of personal data without permission; and
  - loss of availability of personal data.
- The school needs to ensure that there are robust systems in place to detect, investigate and report any personal data breaches.
- The UK GDPR makes it clear that when a security incident takes place, we are required, as a matter of urgency, to establish whether a personal data breach has occurred and, if so, promptly take steps to address it. Some data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job whilst other breaches can significantly affect individuals whose personal data has been compromised. This needs to be assessed on a case-by-case basis.
- Under the UK GDPR we are required to report a personal data breach to the ICO within 72 hours, when it is felt that as a result of that breach there is likelihood of a risk to people's rights and freedoms. A breach can have a range of adverse effects on individuals which might include emotional distress and/or physical and material damage.
- Where it is not felt that this risk is likely, it is not necessary to report the breach, but we will still document the breach and justify the decisions that have been taken, together with any subsequent action
- Where the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms we will inform those individuals without undue delay.
- When reporting a breach, we are required to provide the UK GDPR with the following information:
  - a description of the nature of the personal data and, where possible, the categories and number of individuals concerned together with the category and number of personal date records concerned
  - the name and contact details of our Data Protection Officer
  - a description of the likely consequences of the personal data breach; and
  - a description of the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects.
- See Appendix 5 for more detailed information on the process of reporting data breaches as well as from the ICO's website.[4]
- We will keep records of any data breach, whether or not we are required to inform the ICO.

[4] ICO's guidance to reporting a data breach

- At the start of their employment Staff are required to read and sign a Secure Handling and Acceptable Use of ICT Policy to confirm that they understand of the do's and don'ts of the handling of data and the use of school IT.

**11. <u>Securing and Handling Data</u>**

- All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them. This will be the responsibility of the Head Teacher of Princecroft School.
- All staff understand that they must use the school's ICT systems in a responsible way to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users.
- All staff will follow the procedures laid out in their staff code of conduct regarding both secure data handling and use of the internet.
- If a member of staff believes that the data on any device is breached they must report it to a member of the SMT.
- All personal or commercially sensitive data (pupil records, SEN data, contact details, assessment information) will be backed up, encrypted and stored in a secure place – e.g. safe / fire safe / remote backup. This includes data held on fixed computers, laptops and memory sticks. When required the Schools' ICT support should be contacted to facilitate encryption of devices.
- Staff should **<u>not</u>** remove or copy sensitive data from the organisation or authorised premises unless the media is:
  - encrypted,
  - is transported securely
  - will be stored in a secure location
- This type of data should not be transmitted in unsecured emails (e.g. pupil names and addresses, performance reviews etc).
- 'School to school'[5] and internal exchange of data should be done via email or paper, providing a link to the location of data on the secure server. Alternatively, data transfer should be through a secure encrypted email system e.g. S2S, SecureNet Plus, common transfer files and school census data. If this is not available then the file must, as a minimum precaution, be password protected before sending via email. The password must be sent by other means and on no account included in the same email.
  A record of the email should be kept, to identify when and to whom the email was sent, (e.g. by copying and pasting the email into a Word document). Never put personal information such as pupils' names in the subject line of any email.
- 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 the ICT Support Technician using a recognised tool.
- The school's wireless network (WiFi) will be secure at all times.
- The school will identify which members of staff are responsible for specific data protection. The school will ensure that staff who are responsible for sets of information, such as SEN, medical, vulnerable learners and management data know what data is held, who has access to it, how it is retained and disposed of. This is shared with all staff concerned within the school.
- Where a member of the school staff 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. **<u>This information must not be stored on a personal (home) computer.</u>**
- Members of staff (e.g. SMT) who are given full, unrestricted access to an organisation's management information system should be aware that higher grades of sensitive data is accessible. **<u>This information must not be stored on a personal (home) computer.</u>**

[5] School to school service: how to transfer information (DfE March 2014)

- The school will keep necessary pupil and staff information in accordance with the guidance from the Department of Education and as stipulated in the school's own audit.
- When no longer required, the school should securely delete commercially sensitive or personal data as outlined in its audit.

**12. Freedom of Information**

The school understands its obligations under the Freedom of Information Act 2000 and the procedures which need to be followed. The policy and procedures are published on the school web site

**13. Policy Review**

This policy will be reviewed every two years or earlier in the event of any changes to legislation.

**APPENDIX 1 - ICO NOTIFICATION OF SECURITY BREACHES**

Data protection legislation incorporates a requirement for a personal data breach to be notified to the supervisory authority and in some cases to the affected individuals. A data breach will be notifiable when it is deemed by the school as likely to pose a risk to people's rights and freedoms. If it does not carry that risk, the breach is not subject to notification although it will be entered on the school's breach record.

**Timescales for notification to supervisory authority**

Where a notifiable breach has occurred, the school will notify the Information Commissioners Office (ICO) without undue delay and at the latest within 72 hours of it becoming aware of the breach. If notification is made beyond this timeline, the school will provide the ICO with reasons for this.

If it has not been possible to conduct a full investigation into the breach in order to give full details to the ICO within 72 hours, an initial notification of the breach will be made within 72 hours, giving as much detail as possible, together with reasons for incomplete notification and an estimated timescale for full notification. The initial notification will be followed up by further communication to the ICO to submit the remaining information.

**Content of breach notification to the supervisory authority**

The following information will be provided when a breach is notified:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the Data Protection Officer where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

**Timescales for notification to affected individuals**

Where a notifiable breach has occurred which is deemed to have a high risk to the rights and freedoms of individuals, the school will notify the affected individuals themselves i.e. the individuals whose data is involved in the breach, in addition to the supervisory authority. This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

**Content of breach notification to the affected individuals**

The following information will be provided when a breach is notified to the affected individuals:

- a description of the nature of the breach;
- the name and contact details of the Data Protection Officer where more information can be obtained;
- a description of the likely consequences of the personal data breach; and

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

**Record of breaches**

The school records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under data protection legislation. It records the facts relating to the breach, its effects and the remedial action taken.

**APPENDIX 2 - DATA SUBJECT ACCESS REQUESTS – FREQUENTLY ASKED QUESTIONS**

We have answered the key questions below, however much more detail can be found on the ICO's website regarding an individual's right to access.

**1. Making a subject access request?**
A Subject Access Request (SAR) must be made in writing (which can include an email or social media). If a request is made verbally, there is no obligation for the school to respond however, depending on the circumstances, we may still be happy to do so but will advise you of this at the time.

Where the individual requesting the data is disabled and as a result finds it extremely difficult to make the request in writing, we are happy to make an adjustment for them in line with our obligations under the 2010 Equality Act. We will also take into account their specific disability in the way in which we respond.

A request form is provided in this appendix for making a request, though making a request in this format is not a requirement. Including specific details of the data you wish to see in your request will enable a more efficient response. We may need to contact you for further details on your request if insufficient information is contained in the original request.

**2. What about when the SAR is made on behalf of another individual?**
The law does not prevent you from making a subject access request via a third party. This might be a solicitor acting on your behalf or simply a friend or relative, if this makes you feel more comfortable. However, you must provide written authority and the school reserves the right to contact you should we have any concerns about the request and/or supplying the data to your representative.

**3. What if I want to request information about my child who is a pupil at the school?**
Where you are making a SAR on behalf of a pupil (in your care) the legal position is that the data (whatever their age) is still their personal data and does not belong, for example, to a parent or guardian. It is the child therefore who has the right of access, even though in the case of young children these rights are likely to be exercised by those with parental responsibility.

Before we respond to a SAR for information held about a child, we are entitled to consider whether or not the child is mature enough to understand their rights and, if we are confident that this is the case, we are legally required to respond to the child. In England there is no legal age limit at which it is presumed that a child is mature enough (although the age in Scotland is set at 12, which may be a

reasonable indication of appropriate age. When considering borderline cases, we are required to take other factors into consideration, namely:

- the child's level of maturity and their ability to make decisions like this
- the nature of the personal data
- any court orders relating to parental access or responsibility that may apply
- any duty of confidence owed to the child or young person
- any consequences of allowing those with parental responsibility access to the child's of young person's information: this is particularly important if there have been any allegations of abuse or ill treatment
- any detriment to the child or young person if individuals with parental responsibility cannot access the information, and
- any view's the child or young person has on whether their parents should have access to information about them.

**4. What happens if the data I am asking for also includes information about other people?**

If, by disclosing the information you request would also mean disclosing information about another individual who can then be identified, we do not have to comply with your request except where the other individual has consented to us supplying the information or we believe that it is reasonable, taking into consideration all the circumstances, to comply without the other individual's consent.

**5. Can I be asked for more information when I make a SAR?**

We are allowed to confirm two things with you when you make a SAR:

1. If we are in any doubt about the identity of someone requesting information on personal data, we are allowed to request more details from you to ensure that we are not giving personal data out to the wrong person.
2. We may also need further information from you to ensure that we find the data that you have requested and where this is the case, the time limit will start from the date on which we receive the additional information.

**6. Will I have to pay a fee and if so, how much?**

Generally a fee is not payable for a SAR. A charge may be applied if the request is excessive or repetitive. In addition, we may charge a reasonable fee if you request further copies of the same information. The fee charged will be based on the administrative cost of providing the information requested. If the SAR is made for information on a pupil's 'educational record', we must provide a response within 15 school days. If it does not relate to any information that forms part of the educational record, then we have the usual one month time limit for responding.

**What about repeated or unreasonable requests?**

Whilst the Data Protection Act does not limit the number of SAR you can make, it does allow some discretion when dealing with requests that we believe to be made at unreasonable intervals. We are not obliged to comply with identical or similar request to one you have already made unless a reasonable amount of time has passed between the first request and any subsequent requests. When deciding on whether or not requests are made at reasonable intervals, we can take the following factors into consideration:

- the type of data and whether or not it is particularly sensitive
- the purpose of us processing the data and whether or not it is likely to be detrimental to you as an individual, and
- how often the data is altered as if it changes frequently, it would not be unreasonable for requests to be closer together in terms of when they are made.

**SUBJECT ACCESS REQUEST FORM**

Once completed, please submit this form to the Data Protection Officer (DPO) at: admin@princecroft.wilts.sch.uk or post it to Data Protection Officer, Princecroft Primary School, Princecroft Lane, Warminster, Wiltshire, BA12 8NT.

| **Personal details** | |
|---|---|
| Your name: | |
| Person category *e.g. employee (past or present), pupil, parent*: | |
| Telephone number: | |
| Email address: | |
| Home address: | |
| **Information sought** | |
| Please use the space below to describe, in as much detail as possible, the information you wish to have access to. If appropriate, please include any dates relevant to the information sought. | |
| **Declaration** | |
| I confirm that I am the person named above and the information requested above is in relation to me. I understand that I may be required to provide evidence to verify my identity. | |
| **Your signature:** | |
| **Date:** | |

**APPENDIX 3- INFORMATION ASSET / DATA REGISTER / SECURE DATA HANDLING**

The school must manage records effectively, in compliance with data protection and other regulation. As a school we collect, hold, store and create significant amounts of data and information and this register provides a framework of retention and disposal for categories of information and documents.

We are committed to the principles of data protection including the principle that information is only to be retained for as long as necessary for the purpose concerned.

The Head Teacher is responsible for ensuring that this is carried out appropriately.

**APPENDIX 4 – DATA RECTIFICATION REQUEST FORM**

**DATA RECTIFICATION REQUEST FORM**

Once completed, please submit this form to the Data Protection Officer (DPO) at: admin@princecroft.wilts.sch.uk or post it to Data Protection Officer, Princecroft Primary School, Princecroft Lane, Warminster, Wiltshire, BA12 8NT.

| **Personal details** | |
|---|---|
| Your name: | |
| Your status *e.g. employee, pupil etc.*: | |
| Telephone number: | |
| Email address: | |
| Home address: | |
| **Data you wish to be rectified** | |
| Please use the space below to describe, in as much detail as possible, the data which you believe to be inaccurate or incomplete.<br><br>Please use the space below to describe, in as much detail as possible, the amendments or additions you wish to be made to the data. | |
| **Declaration** | |
| I confirm that I am the individual named above and the information requested above is in relation to me. I understand that I may be required to provide evidence to verify my identity. | |
| **Your signature:** | |
| **Date:** | |

**APPENDIX 5 – DATA DELETION REQUEST FORM**

**DATA DELETION REQUEST FORM**

Once completed, please submit this form to the Data Protection Officer (DPO) at: admin@princecroft.wilts.sch.uk or post it to Data Protection Officer, Princecroft Primary School, Princecroft Lane, Warminster, Wiltshire, BA12 8NT.

| **Personal details** | |
|---|---|
| Your name: | |
| Your status *e.g. employee, pupil etc.*: | |
| Telephone number: | |
| Email address: | |
| Home address: | |
| **Data you wish to be deleted** | |
| Please use the space below to describe, in as much detail as possible, the data which you wish to be deleted.<br><br>**Reason for request**<br>Please indicate below which of the reasons set out above applies to your request | |
| **Declaration** | |
| I confirm that I am the individual named above and the information requested above is in relation to me. I understand that I may be required to provide evidence to verify my identity. | |
| **Your signature:** | |
| **Date:** | |