Princecroft
PRIMARY SCHOOL

Incorporating The Hive Nursery

Acceptable Use and Secure Data Handling Policy

Issue date	
Review date	Nov 2018
Date of next policy review	Nov 2021

This policy is in line with the Single Equality Policy

Princecroft Primary School
Princecroft Lane
Warminster
Wiltshire
BA12 8NT

Headteacher: Michael Park

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

Acceptable Use of ICT and Secure Data Handling Policy

This policy should be read and understood in conjunction with the following policies and guidance:

- The Data Protection Act 2018
- Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2008
- Records Management Society – Tool Kit for Schools

Principles:

Schools have increasing access to a wide range of sensitive information. There are generally two types of sensitive information; personal data concerning the staff and pupils and commercially sensitive financial data. It is important to ensure that both types of information are managed in a secure way at all times.

Personal data is the most likely form of sensitive data that a school will hold. Personal data is defined by the Data Protection Act as ***"Data relating to a living individual who can be identified from the data*****".** The Act gives 8 principles to bear in mind when dealing with such information. Data must:

1. be processed fairly and lawfully
2. be collected for a specified purpose and not used for anything incompatible with that purpose
3. be adequate, relevant and not excessive
4. be accurate and up-to-date
5. not be kept longer than necessary
6. be processed in accordance with the rights of the data subject
7. be kept securely
8. Not be transferred outside the EEA (European Economic Area) unless the country offers adequate protection.

The Data Protection Act states that some types of personal information demand an even higher level of protection, this includes information relating to:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life (orientation)
- The commission or alleged commission by them of any offence, or any proceedings for such or the sentence of any court in such proceedings.

The three questions below can be used to quickly assess whether information needs to treated securely, i.e.

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

If the answer to any of the above is “yes” then it will contain personal or commercially sensitive information and needs a level of protection. (A more detailed assessment guide is contained with Appendix A).

Procedures and practice:
The following practices must be applied within the school:

- The amount of data held by the school should be reduced to a minimum.
- Data held by the school must be routinely assessed to consider whether it still needs to be kept or not.
- Personal data held by the school will be securely stored and sent by secure means.

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

- A register (Appendix B) must be kept detailing the types of sensitive 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.
- Audits will take place in line with the timetable. (Appendix C).

This register must be sent to all staff each year to allow colleagues to revise the list of types of data that they hold and manage.

The audit will be completed by a member of staff responsible for data protection

Risk assessment:
If it has not already been undertaken, 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.

Carrying out a risk assessment will generally involve:

- 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?

Once the risk assessment has been completed, the school can decide how to reduce any risks or whether they are at an acceptable level.

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.

Securing and handling data held by the school:
The school will encrypt[1] any data that is determined to be personal or commercially sensitive in nature. This includes fixed computers, laptops and memory sticks. The ICT support should be contacted to facilitate encryption of devices.

Staff should **not** 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).

Data transfer should be through secure websites e.g. S2S, RPowered, Perspective Lite and common transfer files.

The school's wireless network (WiFi) will be secure at all times. Use of the school's Wi-Fi is not permitted for governors and visitors.

The school will identify which members of staff are responsible for data protection. The school will ensure that staff who are responsible for sets of information, such as SEN, medical, vulnerable learners, management data etc. know what data is held, who has access to it, how it is retained and disposed of. Appendix C details which members of staff are responsible for which data. This is shared with all staff concerned within the school.

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.**

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.**

The school will keep necessary pupil and staff information in accordance with the Records Management Society's guidance.

The school should securely delete commercially sensitive or personal data when it is no longer required as per the Records Management Society's guidance.

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 headteacher.

When sensitive data is to be sent out of the school it must be done in a secure way.

---

[1] Encryption of computers and memory sticks can be provided by the school's technical support.

This Policy will be reviewed every three years or earlier if required.

APPENDIX A: Help sheet for assessing risk of sharing information

In deciding the most appropriate way to share information and the level of security required, you must always take into consideration the nature of the information and the urgency of the situation, i.e. take a risk based approach to determining appropriate measures.

The simplified process described below will help organisations to choose the appropriate level of security to consider when emailing information.

Step 1
Imagine a potential security breach (e.g. a confidential letter is left in a public area, a memory stick is lost or someone reads information on a computer screen while waiting to meet a member of staff), and consider:

1 Will it affect or identify any member of the school or community?
2 Will someone lose / be out of pocket by / more than £100?
3 Will it cause any kind of criminal case to fail?
4 Is there a risk of discomfort / slur upon professional character of someone?
5 Is anyone's personal safety at risk?
6 Will it embarrass anyone?

If you answered **NO** to all the questions, the document does not contain sensitive information. If you answered yes to any of the questions, the document with include some sensitive information and therefore requires a level of protection.

Step 2
Imagine the same potential security breach as above, and consider:

7 Will it affect many members of the school or local community and need extra resources locally to manage it?
8 Will an individual or someone who does business with the school lose / be out of pocket by £1,000 to £10,000?
9 Will a serious criminal case or prosecution fail?
10 Is someone's personal safety at a moderate risk?
11 Will someone lose his or her professional reputation?
12 Will a company or organisation that works with the school lose £100,000 to £1,000,000?

If you have answered **yes** to any of the above questions the document contains sensitive information and additional security should be considered, such as, password protecting the document before you email it to a colleague outside of your organisation.

However, if you think that the potential impact exceeds that stated in the question (for example, someone's personal safety is at high risk) think very carefully before you release this information.

Step 3

All documents that do not fit into steps 1 or 2 might require a higher level of protection / security; organisations should err on the side of caution

Appendix B: Register of sensitive data held by the school

Type of data	Held on	Period to be retained	Type of protection	Who can access the data

Appendix C: Timetable for Information Security Management

Activity	**Frequency**	**Lead**
Audit of data held	Annually	Head and admin officer
Encrypting sensitive data	On-going	All staff
Reviewing data backup procedures	Annual	Admin officer/IT Support
Identifying staff responsible for data security and keep log of names and roles.	Annual	Head
Wiping of laptop data when re-issued	Annual and then when necessary.	ICT Technician
Wiping of laptop data when discarded	As necessary	ICT Technician

Appendix D

This policy is reviewed every two years or as necessary

Staff Secure Data Handling and Acceptable Use of ICT Policy

School Name Princecroft Primary School

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system and resources in a professional, lawful and ethical manner. To ensure that all members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Secure Data Handling and Acceptable Use of ICT Policy.

This is not an exhaustive list and all members of staff are reminded that ICT should be consistent with the school ethos, other appropriate policies and the law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDA's, laptops, tablets, digital cameras, smart devices, email and social media sites.

- School owned information systems must be used appropriately. I understand that the computer misuse act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware or software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a strong password (A strong password has numbers, letters and symbols with 8 or more characters, does not contain a dictionary word and is only used on one system).

- Screens of PC's, laptops and ipads must be locked when not in use

- I will not permit anyone to use my IT devices under my login.

- I understand that I am responsible for all activity carried out under my user name.

- I will not use anyone else's login account.
- I will ensure that any electronic device that I use will lock automatically if an incorrect password is entered after several attempts.
- I understand that I must lock portable electronic devices in a locked cupboard at the end of the working day.
- I understand that school devices may not be used by anyone other than the person that they are issued to.
- I will save documents to the server and not to the desktop or local drives.
- I will ensure that data is kept securely and is used appropriately at all times.
- I will report the loss of a device used for work related activities immediately to the Head Teacher.
- All staff and governors must only use the approved email system for the school.
- I will password protect documents that are sensitive and/or contain personal information.
- 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.
- I will not send sensitive and/or personal information in an email. Instead I will send a password protected document and call the recipient with the password.
- I will request the ICT support apply permissions appropriate to sensitive and or personal folders.
- All USB sticks must be encrypted and issued by the school.
- I acknowledge that the computer provided for me to use remains the property of the school and should only be used for school business.
- I will not access the files of others or attempt to alter the computer settings.
- I will not update web content or use pictures or text that can identify the school, without the permission of the Head Teacher.
- 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.
- I understand that the school may 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 Network Manager / school technician / head teacher.
- Any e-mail messages I send will not damage the reputation of the school.
- I understand that all joke e-mails and attachments are potentially damaging and undesirable and therefore must 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 sensitive data files and no secure electronic option is available I will only do so using the encrypted USB key provided by the school.
- Sensitive data must only be sent electronically through a secure method, e.g. Secure Net Plus. If this is not available then the minimum requirement is to password protect the document before attaching it to email.

  Sensitive data includes:
  - Pupil reports
  - SEN records
  - Letters to parents
  - Class based assessments
  - Exam results
  - Whole school data
  - Medical information

- Information relating to staff, e.g. Performance Management reviews.

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 will not attempt to install any hardware or software including browser toolbars on any school owned devices without permission from the IT systems manager.

- I understand that I must not download unverified apps that may present a threat to security on my devices.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. All personal data will be obtained and processed fairly and lawfully, only kept for the specific purpose that it was obtained, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online(only with countries or sites with suitable data protection controls), or accessed remotely. Any data which is being removed from the school site such as via email, memory sticks or CDs must be encrypted by a method approved by the school. Encrypted USB sticks must be obtained from the School Business Manager who will register the device and who it was issued to. The device must be returned when no longer required or when the staff member leaves and the information wiped. Any images or videos of pupils will only be used as stated in the Data Protection policy and will take into account parental consent.

- I will not use any personal device for school business.

- I will not keep professional documents which contain school related sensitive or personal information (including images, files, videos etc. on **any** personal device such as laptops, digital cameras, mobile phones, I pads). I will protect devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- Personal mobile phones or digital cameras must never be used for taking any photographs related to school business. The school should have a camera specifically for this purpose. The school camera must never be used for personal use.

- Images will only be taken, stored and used for purposes within the school unless there has been permission from parents for an alternative use. Parental consent is to be requested at the start of each school year for taking children's photos and for using their children's image in the school brochure and the local press. The school will not use any images where approval has not been given by the parent/carer. Filming and photographing of children at school events such as sports days and school productions are not permitted. Images of children must be stored on the secure server.

- I will respect copyright and intellectual property rights.

- I have read and understood the school's e-safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I understand that I must report any incidents of concerns regarding staff use of technology and/or children's safety to the Head or the Deputy Designated Professional in line with the school's safeguarding policy.

- I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-safety coordinator or the Business Manager.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus I will report this to the Head Teacher and the Business Manager as soon as possible.

- I understand that I must not use unsecured networks.

- My electronic communication with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email addresses or telephone number. Any pre-existing relationships which may compromise this must be discussed with the safety coordinator.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not

interfere with my work duties and will be in accordance with the school policies and the law.

- I will not create, browse, download, upload, transmit, display, publish or forward any material that is likely to be considered offensive, illegal, discriminatory, harassment, inconvenience or needless anxiety to any other person or anything which could bring my professional role, the school or the County Council, into disrepute.

- I will promote e safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content that they access or create.

- If I have any queries or questions regarding safe and professional practice online either in school or off site then I will raise them with the Ethos and Welfare Governors or the Head Teacher.

- I understand that it is a disciplinary offence to use the Information Systems for any purpose not permitted by the school. IT usage, internet and email may be monitored to ensure policy compliance and inappropriate use could lead to disciplinary proceedings. The Head Teacher should be asked for clarity if there is any doubt of what is permitted.

- If an E safety incident should occur staff must report it to the designated member of staff(s) for child protection as soon as possible.

- The school Wi-Fi must be kept secure and the code not given to governors or visitors

- I understand that all school devices must be returned to the school at the end of my employment.

- I understand that hard copy personal and or sensitive data must be kept secure at all times. It must not be left unattended and must be locked away securely.

- Any hard copy data that is taken off of the school site must be authorised by the Head Teacher and must be transported and kept secure.

- I must not disclose any personal and or sensitive data to anyone that is not authorised to receive it.

- In the event that hard copy data is lost I will immediately inform the Head Teacher.

- Hard Copy data must be retained as instructed in the IRMS toolkit for schools. The School Business Manager will have this information

- Hard Copy sensitive data must be transferred by secure means and proof of receipt must be obtained.

The school may exercise the right to monitor the use of information systems, including internet access and the interception of emails in order to monitor compliance with this acceptable use policy and the schools Data Protection Policy. Where it believes unauthorised and/or inappropriate use of the services information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound the matter will be bought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with the Secure Data Handling and ICT Acceptable Use Policy

Signed……..

Print Name……

Date…….