2018

HURLEY PRIMARY SCHOOL

INFORMATION SECURITY POLICY

CONTENTS

1. Scope

This Policy applies to:

- All members of staff, governors [and trustees] ; “Staff” includes all employees, locum staff, volunteers, work experience and any other individuals working for Hurley Primary School on a contractual basis.

The Importance of this Policy:

- This information Security Policy lets you know what your Information Security responsibilities are at Hurley Primary School; everyone has a role to play and it’s vital you understand yours.

The Objective of this Policy is to:

- Inform staff, governors [and trustees] and protect Hurley Primary School from security issues that might have an adverse impact on our organisation. Achieving this objective will rely on all staff, governors [and trustees] of the Hurley Primary School complying with this policy.

2. Key Principles

The Hurley Primary School has adopted the following six principles to underpin its Information Security Policy:

All Personal data shall be:

(1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

(2) used for specified, explicit and legitimate purposes ('purpose limitation');

(3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');

(5) kept no longer than is necessary ('storage limitation');

(6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

3. Creating, storing and managing information

Hurley Primary School has adopted both a Clear Desk and Clear Screen Policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when work areas and computers are unattended.

The purpose of this section is to establish Hurley Primary School’s requirements to ensure that information is not disclosed by being made available in any form to unauthorised individuals.

3.1 Paper information

● Keep clear desks as this is an obvious way of preventing any confidentiality problems arising from having pupils or other staff members at desks, or disclosure when desks are left unattended. A clear desk will help to protect against the disclosure of information.

● Confidential documents must not be left on display or unsupervised.

● Store confidential information in locked cabinets, returning them to these cabinets when not required.

● Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids.

● Do not leave paper by printers or photocopiers where other people may take it or read it accidentally.

● Spoiled photocopies and prints may still be confidential. Do not put them straight into the waste paper bin, dispose of them as confidential waste. Always check that originals have been removed from the device as well as copies.

● Dispose of confidential paper by shredding or put in a confidential waste bag and follow confidential waste disposal procedure. Do not dispose of confidential waste in a waste paper bin or anywhere else.

● Destroying information earlier than necessary may be a breach of the law so it is important that retention periods are checked before destroying any records.

3.2 Electronic information

● All confidential information must be stored on Hurley Primary School approved electronic devices or systems with access controlled/restricted, e.g. the Hurley Primary School network, Google drive with appropriate restricted access Hurley Primary School approved systems.

● Confidential information must not be stored on local unencrypted hard drives.

● If confidential information has to be transferred to other portable media, such as USB stick or memory cards, it must be encrypted with appropriate security software approved by Hurley Primary School.

● PC screens/laptops/tablets must be sited away from public areas so that pupils and visitors cannot read the screens, e.g. through windows or while waiting in public areas.

● Notebook PCs, handhelds or any other portable ICT device must not be left unattended in any public area (see Mobile Computing below).

● Individual user id/passwords must not be shared with anyone, including other staff members and governors, and do not use anyone else's password. You as an individual are responsible for all transactions undertaken on the Hurley Primary School network using your network id.

● Passwords must not be written down and left with any equipment or accessible by anyone else.

● Make passwords hard for anyone else to guess by incorporating numbers and mixed case into it. Some systems will force this already.

● Lock screens whenever leaving any ICT equipment unattended. This will prevent anyone accessing any restricted information on the equipment while it is unattended.

● If you find you have access to confidential information that you believe should be restricted, you should notify Hurley Primary School immediately.

4. Receiving, sending and sharing information

4.1 Post – receiving and sending

● Post should be opened and dealt with away from public areas and securely, if dealing with confidential information. Do not leave unsealed confidential documents in open post trays and 'pigeon holes'.

● Staff must ensure that any mail to an individual marked: Private, Confidential or Personal, or any combination, is only passed to the named recipient unless a prior delegation arrangement has been made.

● If outgoing post contains confidential information to an individual, the envelope should be marked as 'Private and confidential' and 'to be opened by addressee only'. A return address must be shown on the envelope and you should consider double bagging the package.

● Print each letter separately making use of any printing security and use window envelopes. Check the address is the current, correct one – don't copy previous letters. Double check that the letter and papers are for the correct recipient and address.

● When using a mailshot or multiple mailings, have a procedure in place to check you haven't included anyone else's personal information in the wrong envelope. Another person or supervisor should check mailings against address lists and sign-off before dispatch.

● Consider using signed for/tracked post, if it contains sensitive or confidential documents and/or the volume justifies secure delivery.

● Post containing very high risk/Confidential-Restricted information should only be sent to a named person and use of tracked and signed for mail or a courier to deliver to the name person with signature of receipt.

● If post goes astray or is issued to the incorrect address, notify your line manager immediately and if the information contains personal or confidential information report using the security incident procedure.

4.2 Email and Other Electronic Communications (e.g. text messages) – receiving and sending

● Hurley Primary School does not have total control over emails received, so staff must be aware of the dangers of opening messages from unknown or untrusted sources. Do not click on links in emails unless you know they are from a trusted source and never provide passwords in response to email requests.

● If you are not the intended recipient, the sender should be informed that the message has not reached its intended destination and has been deleted.

● Check the email address is the correct one – there are staff with similar names and your email contacts will also have external email contacts. Double check that the email is for the correct recipient before sending.

● If sending to a list/group of parents or others, send using 'blind copy' (bcc) so the recipients are not copied in to a large list. This especially applies to mailshots.

● Confidential and Confidential-Restricted information must not be emailed externally using normal email unless;

a) you are using an encrypted email service provided by Hurley Primary School or

b) the information is encrypted / password protected in an attachment, or

c) you are sending to an approved Hurley Primary School email address, e.g. a school welearn email address, or

d) you are sending to an e-mail address which utilises the same server – for schools which use the 'welearn' e-mail system this includes all other schools with this system as well as Warwickshire County Council.

● Records of personal data sent by email or other electronic communications (internal or external) are accessible to the data subject if they request access under the GDPR. If a permanent record is required they should be saved to the appropriate file and the email removed from the email inbox. Do not use personal email as a permanent filing system for pupil, parent or staff records. When a member of staff leaves or moves to another job, the line manager must go through the Leavers Checklist and save and secure any emails needed to be kept Hurley Primary School records.

● Hurley Primary School Confidential email must not be forwarded to your own personal email account for private use.

4.3 Telephone calls

● Ensure that you are talking to who you think you are speaking with by verifying their details. It may be appropriate to call them back to verify their credentials.

● If it becomes necessary to leave the phone for any reason, put the caller on hold so that they cannot hear other potentially confidential conversations that may be going on in the office.

● If the call received or being made is of a confidential or sensitive nature, consider who else may be listening to the conversation.

● If a message needs to be taken and left on someone's desk, ensure that these messages do not themselves contain confidential information.

● Do not leave confidential messages on an answer machine as these can be reviewed by people other than the intended person.

4.4 Conversations

Staff should remember that even though they may be on Hurley Primary School premises there may be pupils and visitors around.

● When having a meeting or interview with someone where confidential information will be discussed, ensure that there is sufficient privacy. Check that the room is suitable.

● Confidential information should only be discussed with colleagues who need to know the information in order to carry out their job.

● Always consider your surroundings and the proximity of others who may be able to hear in public places.

4.5 Information sharing/processing

When confidential or personal data is shared with other agencies, for example with local authorities or external providers, then arrangements must be made for that information sharing to be done in a controlled way that meets ethical and legal obligations in one of two ways:

1. If a service is commissioned with an external provider that needs confidential information to operate then the contract must contain clauses that list the commissioned organisation's responsibilities for confidential and personal data, including data protection and security. This must include whether the organisation is processing personal data on behalf Hurley Primary School or has sole or joint responsibilities for the personal data with Hurley Primary School. All staff involved in such data commissioning/sharing must be aware of the details of any existing information sharing agreements/contractual agreements and the obligations that it places on them.

2. If information has to be shared with another organisation on a regular basis for legal reasons then this should be done under an information sharing agreement that sets out how the sharing will operate and the standards of management that all parties to the agreement must comply with. Such an agreement will define exactly what information will be shared and how, including the method, transmission or communication between agencies or any shared access security arrangements. The aim is to ensure that appropriate arrangements operate in the participant agencies and ensure the continued confidentiality of shared information. If staff are unclear on what basis information is being shared with another agency, whether an information agreement exists and what obligations that might place on them, it should be clarified with their manager.

5. Working Away from School

The purpose of this section is to ensure that information assets and information processing facilities, used to access personal and confidential information, are adequately protected with logical, physical and environmental controls.

This includes working away from the school, at home and use of own devices to access personal and confidential information.

Work-related information must not be kept permanently at home. Wherever staff are working on, or in possession of, work-related information they are responsible for it, e.g. in school, on the phone, at home, en route to or from school or home, at meetings, conferences, etc. If confidential information is handed out in conferences or meetings, the same person is responsible for collecting it back in at the end, or ensuring it is only in the hands of those authorised to keep it.

- Take only the confidential papers/files with you that you need and keep out of sight in a bag, do not carry around loose or in clear folder.

- Managers must ensure a log is kept of which confidential paper case files/records staff are taking from school and when they are returned.

- Store confidential paper files/records securely in an envelope or bag. Try to use electronic files on an encrypted device or access via secure connection to the network or approved storage location instead.

● Keeping information in cars: lock away paper files and equipment (laptop/notebook) in the boot, do not leave overnight. Take only the equipment/papers/files with you that you need, leave rest locked away.

● Travelling by public transport: make sure you take all information and equipment when leaving. Be aware of conversations on mobile phone about personal and confidential information.

● Use of Laptops: Only school issued devices may be used. Do not write down passwords/pin numbers. You must not use the 'remember me' option to save user and password details on your device when accessing Hurley Primary School system. Make sure these are unticked and sign out/logout after using a system. Do not save login or passwords if asked. Remember any confidential files opened may be downloaded before closing down your device, so delete them from 'downloads'. If files are not accessed directly (e.g. Google drive format files), then all confidential files must stored and accessed locally via a Hurley Primary School approved encrypted media.

● Working at home: Store paper and equipment securely after use, as you would your own personal valuables. Don't leave open confidential files on a table. Lock screen on laptop/tablet and close down after use. All confidential information must be safeguarded from access, no matter how unintentional, by anyone who has no need to know such as family and friends. This would be an unauthorised disclosure. Don't leave any Hurley Primary School equipment or information in a car overnight at home, bring into the house and secure. Don't bin confidential information at home, bring back into an office for confidential waste disposal. Use strong security on a home WiFi connection.

6. Premises security

● All staff must wear their ID badge on school premises and report losses or thefts immediately to their line manager.

● Make sure that all visitors sign in and out at all times and disclose who they are coming to see. Visitors should be supervised at all times and display a visitor/contractor ID badge.

● Staff should be encouraged to challenge anyone in the school if they do not know who they are, e.g. if they are not accompanied by a member of staff or they are not wearing an ID badge.

● Staff should be aware of anyone they do not know attempting to follow them through a security door and if appropriate be prepared to escort them back to reception if necessary.

● Managers should ensure that all paper based records and any records held on computers are adequately protected. Risk assessments should identify any potential threats and an appropriate risk management strategy should be produced

● Parents and others who do not want to discuss their private matters with a receptionist in a public area should be offered the opportunity to be seen elsewhere.

7. Portable Media Devices

The purpose of this section is to establish control requirements for the use of removable media devices within and across Hurley Primary School. Portable media devices include, but are not limited to USB sticks or memory cards.

● Connection of non- Hurley Primary School -supplied removable media devices to the Hurley Primary School computing infrastructure is only permitted for the purpose of reading files from the device; Hurley Primary School files must not be written to a non-Hurley Primary School -supplied device.

● Staff must not alter or disable any controls applied to any computing device by Hurley Primary School IT Service as part of the deployment of a removable media device.

● Removable media devices must not be used for the primary long-term storage of Hurley Primary School information.

● All information classified as Hurley Primary School Confidential' or 'personal' that is stored on a removable media device must be encrypted.

● Passwords applied to encrypted devices must conform to the minimum standard required stated in section 3.2 Electronic Information of this Policy.

8. Anti-Malware

The purpose of this section is to establish requirements, which must be met by all devices within Hurley Primary School's computing infrastructure, to protect the confidentiality, integrity and availability of Hurley Primary School software and information assets from the effects of malware.

● Unless undertaken by or following instruction from IT support staff, staff must not disable anti-malware software running on, or prevent updates being applied to devices.

● The intentional introduction of viruses to Hurley Primary School's computing infrastructure will be regarded as a serious disciplinary matter.

● Only software that has been authorised by Hurley Primary School can be installed upon Hurley Primary School systems.

● Each member of staff is responsible for immediately reporting any abnormal behaviour of Hurley Primary School computing systems to the Hurley Primary School

● Prior to any encryption, all files must be scanned for and cleaned of viruses before being sent to any third party.

9. Access Control

● Access to information shall be restricted to users who have an authorised need to access the information.

● Users of information will have no more access privileges than necessary to be able to fulfil their role.

● All requests for access to Hurley Primary School computer systems must be via a formal request to your IT Team

● Hurley Primary School reserves the right to revoke access to any or all of its computer systems at any time.

● Users must not circumvent the permissions granted to their accounts in order to gain unauthorised access to information resources.

● Users must not allow anyone else to use their account, or use their computers while logged in with their account.

● Computer screens should be 'locked' or the user logged out before leaving any workstation or device unattended.

● Users should not leave workstations or devices in 'sleep mode' for convenience.

10. Monitoring System Access and Use

The purpose of this section is to establish control requirements for the monitoring and logging of information security related events relating to the use of Hurley Primary School's information and information systems.

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. Hurley Primary School will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy.

Any monitoring will be undertaken in accordance with the Human Rights Act and any other applicable law.

11. Potential breaches of security or confidentiality

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it immediately to School Business Manager immediately.

For losses of equipment or if you believe your email or the network may be at risk, contact the Data Protection Officer Mark Randell immediately on 01926 41217.

If equipment or confidential information has been stolen report to the Police and obtain a crime reference number.

Use the Hurley Primary School procedure to report and record incidents. The form is available for download here: 'report a breach' page of the ICO website and see Appendix 1 below.

If you are aware of a potential incident or if you are not sure whether the issue is a security breach then please complete this form as fully as possible and email to: schooldpo@warwickshire.gov.uk as soon as possible and in any event within 4 hours.

Appendix 1: 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 DPO

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

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

The DPO will alert the headteacher and the chair of governors

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, 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 DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will work out 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 [set out where you keep records of these decisions – for example, on the school's computer system, or on a designated software solution]

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 DPO 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 DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on the school's computer system on the Groupcall GDPR IS software package.

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

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.
Actions we will take if….
Special category data (sensitive information) is accidentally made available via email to unauthorised individuals…
The sender must attempt to recall the email as soon as they become aware of the error
Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

In any cases where the recall is unsuccessful, the DPO 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 DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

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

Approved by: Mr Glyn Morgans – Headteacher

Date: 24th May 2018

Next review due: May 2019

If you have any queries or require further information please do not hesitate to contact us on 01827 872207 or email head2032@welearn365.com

Hurley Primary School, Heanley Lane, Hurley, Nr Atherstone, North Warwickshire, CV9 2HY