Information Security Policy

Contents

1. Scope

This Policy applies to:

- All members of the committee, parents and any other individuals working for Park Hill PTA and Thorns PTA on a volunteer basis.

The Importance of this Policy:

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

The Objective of this Policy is to:

- Inform all members of the PTA committee and volunteers and protect Park Hill PTA and Thorns PTA from security issues that might have an adverse impact on our organisation. Achieving this objective will rely on all members of the Park Hill PTA and Thorns PTA complying with this policy.

2. Key Principles

Park Hill PTA and Thorns PTA have 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

Park Hill PTA and Thorns PTA have adopted both a Clear Desk and Clear Screen Policy to reduce the risk of unauthorised access, loss of, and damage to information when at school and/or at home.

The purpose of this section is to establish Park Hill and Thorns PTA's requirements to ensure that information is not disclosed by being made available in any form to unauthorised individuals.

3.1 Paper information

● Put all information away. This is an obvious way of preventing any confidentiality problems arising and will help to protect against the disclosure of information.

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

● 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.

● All information that has been used for an event must be taken to school and shredded within 30 days of the event ending.

3.2 Electronic information

● All confidential information must be stored on Park Hill PTA and Thorns PTA approved electronic devices or systems with access controlled/restricted, e.g the PTA Gmail accounts.

● 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 and then deleted after each event.

● 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 members and do not use anyone else's password. You as an individual are responsible for all transactions undertaken on the Park Hill PTA and Thorns PTA network using your network id.

● Passwords must not be written down and left with any equipment or accessible by anyone else. PTA email account passwords must be changed yearly.

● 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 Christopher Strelluf (Park Hill) and Claire Bound (Thorns) 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'.

● Committee members and all volunteers 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.

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

● Park Hill PTA and Thorns PTA do not have total control over emails received, so all committee members and volunteers 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 Park Hill PTA or Thorns PTA, or

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

c) you are sending to an approved Park Hill PTA or Thorns PTA email addresses.

● 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 or parent records. When committee members leave they must be taken off the PTA email accounts.

● Park Hill PTA and Thorns PTA 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.

● 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

All Volunteers should remember that even though they may be on Park Hill or Thorns 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 members and volunteers who need to know the information in order to carry out the event.

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

4.5 Information sharing/processing

Confidential or personal data, eg. Information such as age, dietary requirements, is only shared with the people organising each event and the volunteers. This information is needed for the sole purpose of that event. Once the event has finished all this information is shredded at school and deleted from computers.

5. Taking information home

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 at school, at home and use of own devices to access personal and confidential information.

PTA - related information must be kept securely at all times. If information is handed out, the same person is responsible for collecting it back in at the end, or ensuring that 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.

● Store any personal and confidential information 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: No information to be kept in cars

● 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.

● 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 Park Hill PTA and Thorns PTA 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 school for confidential waste disposal. Use strong security on a home WiFi connection.

6. Premises security

● There must be a member of school staff on site for each event.

● All children attending events are either with their parents/carers or have been signed in.

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

7. 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 information on data needed must go through the office.

● 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.

8. Potential breaches of security or confidentiality

If members 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 Christopher Strelluf (Park Hill) or Claire Bound (Thorns).

For losses of equipment or if you believe your email or the network may be at risk, contact Christopher at parkhilljuniorpta@gmail.com and Claire at thornspta@gmail.com