Prince's Trust

The Prince's Trust Information Security Policy

Owner: IT Deptartment

Contents

1. POLICY STATEMENT

This policy aims define how The Prince's Trust ("The Trust") approaches and deals with all aspects of information security to ensure that information remains secure, confidential, accurate and available for its proper purpose.

This policy applies to all The Trust's employees, volunteers and any others working for The Trust (for example casual workers, agency staff and staff on secondment from other organisations). References to 'staff' or 'you' in this policy therefore covers trustees, employees, volunteers and contractors.

Third party companies and delivery partners will have their own policies, but checks should be made that these meet the standards of The Trust's policies. In the event that they do not this policy should be shared with them.

This policy also applies to employees, volunteers and suppliers or delivery partners of Prince's Trust International (PTI) whose IT services are provided by Prince's Trust UK. Failure of PTI to comply with this policy may result in IT services no longer being provided.

This policy should be read in conjunction with the user facing 'Acceptable Use of Information Technology' policy.

Responsibility for this policy rests with The Prince's Trust Council.

2. BACKGROUND

The collection and management of information is a key asset for The Trust and protecting it is vital to our success. Our young people and partners alike rely on us to make sure the information we receive and handle remains safe and secure and complies with the law.

This policy, in conjunction with the 'Acceptable Use of Information Technology' policy and other guidance available on The Loop, define how The Trust approaches and deals with all aspects of information security. The policy and guidance are designed to ensure that information remains confidential, accurate and available for its proper purpose.

The importance of information security cannot be over emphasised. A failure in security controls could easily result in disruption to our work, damage to our reputation, or safeguarding or legal consequences. Even a single incident could seriously damage the reputation of The Trust and affect confidence in our ability to deliver our objectives.

There are 3 basic information security perspectives:

a. Confidentiality: the protection of information from unauthorised disclosure or intelligible interception thus ensuring that the information is only revealed to those with the authority to see or hear it, both inside and outside of The Trust.

b. Integrity: the safeguarding of the accuracy and completeness of information to ensure that the information cannot be modified, inserted, deleted, replayed or otherwise abused, whether accidentally or deliberately.

c. Availability: ensuring that information is available when required by those authorised to have access.

3. OBJECTIVES

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, Applications and networks owned or held by The Trust by:

a) Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other information governance policies.
b) Describing the principles of security good practice and explaining how they are implemented in The Trust.
c) Introducing a consistent approach to security which protects the Information Assets under our control.

4. RESPONSIBILITIES

All Trust personnel, staff, volunteers, or others are responsible for information security and therefore must understand and comply with this and other related policies listed in Section 6 below. All Staff are required to accept responsibility for the actions taken and the things they do and say within their work environment. Information security is the responsibility of each and every person of The Trust.

The Trust monitors all systems and usage of those systems. Where policy breaches have been detected, it may lead to disciplinary processes being undertaken in accordance with HR processes and policies, a volunteer being asked to stop volunteering for The Trust or the termination of a contract with a supplier or contractor.

In addition, there are internal roles where information security responsibilities need to be specifically drawn out. These include:

a) Senior Management – Council and ExCo: The board of trustees (Council) have overall responsibility for security across The Trust. To support this role, Council must include a Senior Information Risk Owner. The Council delegates day-to-day management to ExCo.

b) Senior Information Risk Officer (SIRO): This role is held by the Group General Counsel & Company Secretary and is responsible for both business and information risk for The Trust; their role is to support actions to improve the level of information assurance including risk assessment and risk management throughout The Trust and reports to both ExCo and the Audit & Risk Committee.

c) Chief Technology Officer: Responsible for all aspects of security risk for IT and cyber and security strategy oversight. The scope of this role covers all security technologies and services, including protection services and perimeter defences.

d) IT Security Manager: Responsible the implementation of IT and cyber security management.

e) Safety & Security Manager: Responsible for physical access to buildings and security of buildings.

f) Data Protection Officer (DPO): Responsible for ensuring The Trust complies with data protection legislation.

g) Information Asset Owner (IAO): Every known Information Asset will have a formal IAO, whose role is to understand what information is held, how it is handled, who has access to it and why. They understand and address risks to the information.

h) Technology Committee: acts on behalf of The Trust's Council to ensure information security standards are met.

i) Risk & Audit Committee: acts on behalf of The Trust's Council to ensure information assurance standards are met.

5. POLICY FRAMEWORK

5.1 Certification

The Trust has formal certification in the government backed 'Cyber Essentials' and 'Cyber Essentials Plus' accreditation which will be maintained, giving The Trust technical assurance that we have protection against a wide variety of the most common cyber attacks. We are also working towards benchmarking ourselves against ISO27001, but do not intend to seek formal certification.

5.2 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause.

Information security expectations of staff shall be included within appropriate job definitions and descriptions.

5.3 Access Controls

Access to The Trust's Hardware, Applications, Software, and information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant HR / Information Asset Owner (IAO) / Line manager or member of the IT department.

Access to data, system utilities and programme source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an Application shall depend on the availability of a license from the supplier.

Access to Trust systems must be performed on trust hardware with a network login, with Trust laptops & mobile devices gsecured by a 6-digit PIN to decrypt the device.

External access to email is available to all staff and employees via Microsoft Office 365 and requires additional two-factor Authentication (2FA).

Any approved external access to Trust systems also requires two-factor Authentication (2FA).

5.4 Equipment Security

In order to minimise loss or damage of Assets, the IT Department shall ensure that all electronic equipment and Assets shall be identified, registered and physically protected from threats and environmental hazards.

5.5 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party suppliers working for The Trust.

5.6 Information Risk Assessment

In line with the Data Protection Policy, all information Assets will be identified and assigned an Information Asset Owner. IAO's shall ensure that information risk assessments are performed at least annually, following guidance from the DPO. IAO's shall submit the risk assessment results and associated mitigation plans to the DPO for review.

5.7 Security Incident Management

All security events, near misses, and suspected weaknesses in The Trust's IT security are to be reported to the IT Security manager via the IT helpdesk as soon as possible. Where appropriate this will be reported as an adverse Incident and reported to the DPO, Deputy CIO, CTO and ExCo.

ExCo and the Technology Committee will be updated of all significant incidents through the Monthly Technology Performance Report. The Technology Committee and Risk & Audit Committees will both be notified within 24hours of any major incidents.

Any incidents which involve the loss (or risk of loss) of personal data shall also be reported to the DPO in accordance with the Data Protection Policy.

5.8 Physical Security
All buildings which are owned, occupied, or used by The Trust should maintain good security to protect individuals, Assets and to protect its data. Buildings should have good access control systems in place including CCTV and alarms. Staff members must wear security passes and visitors must be escorted around non-public areas.

5.9 Patch Management

Security patch management is a critical security issue due in large part to the exploitation of information technology systems from numerous external and internal sources. The Trust will maintain a monthly patch cycle across all Hardware, Operating systems, and Applications to ensure all support and security patches are installed within a month of being issued. Patch compliance will be included in the Monthly Technology Performance report to highlight any machines with critical or high impact patches outstanding for more than 30 days.

5.10 Protection from malicious Software

The Trust shall use Software countermeasures and management procedures to protect itself against the threat of malicious Software. All staff shall be expected to co-operate fully with direction from the IT department regarding steps or protective measures to be undertaken.
The 'Acceptable Use of IT' policy defines that users shall not install Software on The Trust's property without permission from the IT department. Users breaching this requirement may be subject to disciplinary or other action.

5.11 Encryption, data transfer and Removable Media

The Trust shall encrypt all its data to 256 bit Advanced Encryption Standard (AES) and be aligned with the Federal Information Standard (FIPS) 140-2.

When information is transferred from The Trust to third-party service providers, to other bodies, commercial organisations, and individuals it must be transferred in a secure manner. All arrangements set out in the Data Protection Policy must be followed, and the transfer method should follow minimum standards approved by the IT department.

The Trust's IT systems automatically encrypt computer storage that is designed to be inserted and removed from its computers' systems. The 'Acceptable Use of IT' policy defines that people should not use Removable Media unless there is a strong business reason

Removable media that contains Software requires the prior approval of its use from the IT department.

Passwords must be used to secure the information using the organisation standard set out in this policy. The password must be sent under a separate mechanism to the encrypted file or Hardware device.

5.12 Acceptable use of IT systems

Staff using The Trust's systems must comply with the Trust's 'Acceptable Use of IT' policy which includes reference to:

- Access Control
- Keeping Control
- Data Protection
- Personal Use of Trust IT
- Monitoring
- Online Content and Social Media
- Use of Trust IT outside your usual workplace
- Avoiding use Removable Media
- Personalisation of equipment

5.13 Computer Access Control and Passwords

Access to The Trust's IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for the protection of their account details and all actions on the The Trust's IT systems in accordance with the 'Acceptable Use of IT' policy.
Passwords must be in place for computers, network and Applications and set against the individual.

Our password policy will ensure that:

- Passwords MUST be changed at first logon
- Passwords MUST be complex:
  - minimum of 8 characters in length
  - differ from their associated user ids
  - And contain a combination of character types: upper case letters, lower case letters, numbers and special characters (e.g. &#%!).
- Passwords MUST be set to expire and changed at regular intervals (maximum 90 days) and that these changes are system invoked.
- Technology MUST restrict the re-use of passwords to the last 5 passwords.

5.14 Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and any unusual activity will be flagged and reviewed on a regular basis.

Appropriate investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The Trust reserves the right to monitor activity on its systems, including internet, email use, and video / voice collaboration tools such as MS teams, and telephone systems in order to ensure systems security, legal requirements, effective operation, and to protect against misuse.

Any monitoring will be undertaken in accordance with the applicable laws and HR procedures.

5.15 Business Continuity and Disaster Recovery Plans

Business impact analysis will be undertaken in all areas of The Trust. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

IT senior management have a responsibility to ensure that appropriate disaster recovery plans are in place for all priority Applications, systems, and networks and that these plans are reviewed and tested on an annual basis.

Incremental backups of all Trust data are performed Monday to Thursday and retained for 1 week before being overwritten.

Full backups of Prince's Trust data are performed as follows:

- Weekly data backed up each week and retained for 4 weeks before being overwritten
- Monthly data backed up each month and retained for 3 months before being overwritten
- Six Monthly data backed up each month and retained for 12 months before being overwritten
- Yearly data backed up yearly and retained in line with the 'Data Retention Policy'.

Recovery points are within 24 hours of failure and recovery times within 48 hours for a single product.

Backups and recovery of data held by our cloud service providers differ and are assessed for alignment with this policy as part of the procurement process.

5.16 Training & Awareness

Individuals will be expected to undertake all mandatory training outlined by their line manager and the Learning and Development Team. IT senior management will work with the Data Protection team and Communications department to issue regular security guidance or security awareness campaigns to raise awareness.

5.17 Forensic Readiness

The Trust and its delivery partners or suppliers must be equipped and have the necessary procedures in place to ensure the collection of digital evidence can be completed to fulfil any legal requirements or procedural internal disciplinary hearings, employment tribunals, arbitration panels and all courts of law if required. The Trust will ensure open and accepted methods for undertaking forensic readiness activities that are both lawful and ethical.

5.18 Clear Desk

All work areas when unattended must be clear of all paper containing person identifiable information, or any other confidential/sensitive information. Such information must be suitably secured. All IT equipment must be password protected when the desk is unattended in line with the 'Acceptable Use of IT' policy. Overnight or for extended periods all equipment and papers should be suitably locked away.

5.19 Remote Working

All Staff have the ability to work remotely using Trust equipment when permitted to do so by their line managers and in line with the 'Acceptable Use of IT' policy. The role must be able to be performed remotely without having an adverse effect on the level and quality of service being provided and in accordance with the Flexible Working Policy (where applicable). Personnel must ensure privacy and confidentiality of The Trust and its Assets is not compromised when working remotely. Papers & equipment should be suitably secured when not in use,

5.20 Supplier Security Requirements

All Suppliers and external organisations must comply to the same security standards at The Trust and pass a security assessment. All third party suppliers and delivery partners should enter into non-disclosure agreements and have data transfer agreement in place (as applicable).

5.21 Prince's Trust International

Prince's Trust UK provides IT services to Prince's Trust International. All Suppliers and external organisations must comply to the same security standards at The Trust and pass a security assessment. All third party suppliers and delivery partners should enter into non-disclosure agreements and have data transfer agreement in place (as applicable).

6. LINKS TO OTHER POLICIES AND GUIDANCE

Other internal policies which may be relevant to this policy are:

Acceptable Use of IT Policy

Data Protection Policy

Joiners and Leavers Policy

Volunteer Policy

Incident Management Policy

Disciplinary Policy

Social Media Policy

Information Security Guidance available on The Loop

7. LEGISLATION

The Data Protection Act (2018)
The General Data Protection Regulation
The Copyright, Designs and Patents Act (1988)
The Computer Misuse Act (1990)
The Health and Safety at Work Act (1974)
Human Rights Act (1998)
Regulation of Investigatory Powers Act (2000)
Freedom of Information Act (2000)
Health & Social Care Act (2012)

8. DEFINITIONS

Application (Software) is a programme or group of Programmes designed for end users. Examples of an Application include a word processor, a spreadsheet, an accounting Application, a web browser, an email client, a media player, a file viewer, simulators, a console game or a photo editor

Asset is a piece of information, Software or Hardware within an information technology environment..

Hardware includes the physical parts of a computer, such as the case, central processing unit, monitor, keyboard, computer data storage, graphics card, sound card, speakers and motherboard. By contrast, Software is the set of instructions that can be stored and run by Hardware.

Operating system is system Software that manages computer Hardware, Software resources, and common services for computer Programmes.

Programmes are a collection of instructions that can be executed by a computer to perform a specific Most computer devices require Programmes to function properly. A computer programme is usually a computer programmer in a programming language.

Removable media is a form of computer storage that is designed to be inserted and removed from a system
Security incident is an adverse event that has caused or has the potential to cause damage to an organisation's Asset, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

Software is a collection of data or computer instructions that tell the computer how to work. This is in to physical Hardware, from which the system is built and actually performs the work.

Source library is a suite of data and programming code that is used to develop Software Programmes and Applications. It is designed to assist both the programmer and the programming language compiler in and executing Software.

System Utility Software is Software designed to help to analyse, configure, optimize or maintain a It is used to support the computer infrastructure - in contrast to Application Software, which is aimed at performing tasks that benefit ordinary users.

9. CONTACTS

Chief Technology Officer

Deputy Chief Information

Officer IT Security Manager

Author	Matt Brentnall
Date approved by Council	21st January 2021
Next review date	21st January 2022