



Pace Independent Special School Information Security Policy

Date Published:	2020	Signed:
Review Date:	April 2021	
This policy must be read in conjunction with:		
<ul style="list-style-type: none">• Data Protection Policy• Data Breach Policy• Data Retention Policy• Electronic Information and Communication Systems Policy• PACE ICT Acceptable use policy agreement		

Contents

Contents	Page 1
Introduction	Page 2
Definition	Page 2
Scope	Page 3
General Principles	Page 3
Physical security and procedures	Page 4
Responsibilities: Members of staff	Page 5
Responsibilities: the on-site IT Technician	Page 5
Access Security	Page 6
Data Security	Page 8
Electronic storage of data	Page 8
Home working	Page 9
Communications, transfer, internet and Mail use	Page 9
Reporting security breaches	Page 10
Appendix: Acceptable use policy agreement	Page 11

Introduction

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the school to achieve this, including to: -

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the School of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

Definition

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Staff are referred to the School's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data.

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

General principles

All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the School's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the Headteacher or Proprietor, who may defer to the on-site IT technician, the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by an onsite IT Admin or by such third party/parties as the Headteacher or Proprietor may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the Headteacher or Proprietor unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the Headteacher or Proprietor who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Physical security and procedures

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available storage rooms, locked cabinets, and other storage systems with locks shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school. The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Headteacher or Proprietor as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

Doors providing access to the building are kept closed to prevent unauthorised access to the building. The building's alarm system is set nightly when the building is locked up. CCTV Cameras are in use at the School and monitored by the Headteacher and the Proprietor.

Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

Responsibilities – Members of staff

- All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.
- Computers and other electronic devices should be locked (CTRL, ALT, Del, Lock) when not in use to minimise the accidental loss or disclosure.
- You must immediately inform the Headteacher or Proprietor of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Notification Policy.
- Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the on-site IT technician immediately.
- You are not entitled to install any software of your own without the approval of the on-site IT technician. Any software belonging to you must be approved by the Headteacher or Proprietor and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.
- Prior to installation of any software onto the IT Systems, you must obtain written permission by the Headteacher or Proprietor. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.
- Prior to any usage of physical media (e.g. USB memory sticks or disks of any kind) for transferring files, you must make sure to have the physical media is virus-scanned. The on-site IT technician approval must be obtain prior to transferring of files using cloud storage systems.
- If you detect any virus this must be reported immediately to the on-site IT technician and the Headteacher or Proprietor (this rule shall apply even where the anti-virus software automatically fixes the problem).

Responsibilities: the on-site IT technician

The on-site IT technician, shall be responsible for the following:

- ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;
- ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the Headteacher and Proprietor, and reporting the outcome of such reviews to the Headteacher and Proprietor;

- ensuring that all members of staff are aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.
- assisting all members of staff in understanding and complying with this policy;
- providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
- ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
- receiving and handling all reports relating to IT Security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing the Data Protection Officer;
- taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
- monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Access security

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teach individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the onsite IT Technician. Biometric log-in methods can only be used if approved by the onsite IT Technician.

All passwords must, where the software, computer, or device allows:

- a) be at least 8 characters long including both numbers, letters and at least one special character;
- b) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the on-site IT technician as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password without the authorisation to do so will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password you should notify the on-site IT technician to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

All mobile devices provided by the School, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Data security

Personal data sent over the school network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Headteacher or Proprietor who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems.

You may have your own devices laptop, connected to the School's Wi-Fi and printer provided that you follow the Headteacher's, Proprietor's and on-site IT technician requirements and instructions governing this use. All usage of your own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy). The Headteacher or Proprietor may at any time request the immediate disconnection of any such devices without notice.

Electronic storage of data

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by on-site IT technician.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any personal data on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the Headteacher or Proprietor. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the School's computer network in order for it to be backed up.

All electronic data is backed up each working day automatically and the success of this is monitored.

Home working

You should not take confidential or other information home without prior permission of the Headteacher or Proprietor, and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

- a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- b) all confidential material that requires disposal is shredded or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.

Communications, transfer, internet and email use

When using the School's IT Systems you are subject to and must comply with the School's Electronic Information and Communication Systems Policy.

The School work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the on-site IT technician and the Headteacher or Proprietor. Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the school cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

Personal or confidential information should not be removed from the School without prior permission from the Headteacher or Proprietor. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

- a) not transported in see-through or other un-secured bags or cases;
- b) not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- c) not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

Reporting security breaches

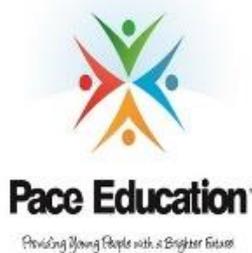
All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the on-site IT technician and the Headteacher or Proprietor. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the Headteacher or Proprietor shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Headteacher or Proprietor. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Headteacher or Proprietor.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Headteacher or Proprietor.

All IT security breaches shall be fully documented. Full details on how to notify of data breaches are set out in the Breach Notification Policy.



PACE ICT Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email) out of school
- I understand that the school ICT systems are intended for educational use, not personal or recreational
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website/Learning Platform) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed by the system administrator
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School's Data Protection Policy and Information Security Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff name:	
Signed:	
Date:	