Information Security Policy

Document provenance

This policy was approved by Trustees as follows –	
Board/Committee: Audit & Risk Committee	Date: 18 May 2018
Frequency of review: 2 years	Next review date: 17 May 2020
ELT Owner: Chris Wiseman	Author: Chris Wiseman

Summary of changes at last review:

- This is a new policy
-
-

Related documents:

- the Trust's privacy notices for staff, pupils and parents
- Data Breach policy
- Information and Records retention policy
- Data Protection Policy; and
- IT acceptable use policy for staff.

1 Introduction

1.1 Information security is about what you and the Trust should be doing to make sure that **Personal Data** is kept safe. This is the most important area of data protection to get right. Most of the data protection fines have come about because of information security breaches.

1.2 The Trust is ultimately responsible for how you handle personal information.

1.3 This policy should be read alongside the Trust's data protection policy which gives an overview of your and the Trust's obligations around data protection. The Trust's data protection policy can be found here http://www.e-act.org.uk/policies. In addition to the data protection policy, you should also read the following which are relevant to data protection:

1.3.1 the Trust's privacy notices for staff, pupils and parents

1.3.2 Data Breach policy

1.3.3 Information and Records retention policy

1.3.4 Data Protection Policy; and

1.3.5 IT acceptable use policy for staff.

1.4 This policy applies to all staff and volunteers (which includes Academy Ambassadorial Group, agency staff, trustees, contractors, work experience students and volunteers) when handling Personal Data. For more information on what Personal Data is, please see the Trust's data protection policy.

1.5 Any questions or concerns about your obligations under this policy should be referred to the Data Protection Officer. Questions and concerns about technical support or for assistance with using the Trust IT systems should be referred to the relevant IT team. Within your Academy or region. Any staff in the national team should refer to the Chief Operating Officer.

2 Be aware

2.1 Information security breaches can happen in a number of different ways. Examples of breaches include:

2.1.1 an unencrypted laptop stolen after being left on the back seat of your car;

2.1.2 Personal Data taken after website was hacked;

2.1.3 sending a confidential email to the wrong recipient; and

2.1.4 leaving confidential documents containing Personal Data unattended on a desk in the office.

2.2 These should give you a good idea of the sorts of things which can go wrong, but please have a think about what problems might arise in your team or department and what you can do to manage the risks. Speak to your line manager and the Data Protection Officer if you have any ideas or suggestions about improving practices in your team. One option is to have team specific checklists to help ensure data protection compliance.

2.3 You should immediately report all security incidents, breaches and weaknesses to the Data Protection Officer. This includes anything which you become aware of even if you are not directly involved (for example, if you know that document storage rooms are sometimes left unlocked at weekends or that staff are continuing to use unencrypted data sticks).

2.4 You must immediately tell the Data Protection Officer, the IT Department and Regional Operations Director if you become aware of anything which might mean that there has been a security breach. You must provide your Regional Operations Director and the Data Protection Officer with all of the information you have. If you cannot get hold of your manager, Regional Operations Director or the Data Protection Officer or it is outside of Academy hours then please use this emergency contact number to contact the Chief Operating Officer: 07808890359. All of the following are examples of a security breach:

2.4.1 you accidently send an email to the wrong recipient;

2.4.2 you cannot find some papers which contain Personal Data; or

2.4.3 any device (such as a laptop or a smartphone) used to access or store Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.

2.5 In certain situations the Trust must report an information security breach to the Information Commissioner's Office (the data protection regulator) and let those whose information has been compromised know within strict timescales. This is another reason why it is vital that you report breaches immediately.

3 Thinking about privacy on a day to day basis

3.1 We should be thinking about data protection and privacy whenever we are handling Personal Data. If you have any suggestions for how the Trust could protect individuals' privacy more robustly please speak to the Data Protection Officer who can be contacted via email on DPO@E-ACT.org.uk.

3.2 From May 2018, the Trust is required to carry out an assessment of the privacy implications of using Personal Data in certain ways. For example, when we introduce new technology, where the processing results in a risk to individual's privacy or where Personal Data is used on a large scale, such as CCTV.

3.3 These assessments should help the Trust to identify the measures needed to prevent information security breaches from taking place. If you think that such an assessment is required please let your Regional Operations Director know.

4 Critical Personal Data

4.1 Data protection is about protecting information about individuals. Even something as simple as a person's name or their hobbies count as their Personal Data. However, some Personal Data is so sensitive that we need to be extra careful. This is called **Critical Personal Data** in this policy and in the data protection policy. Critical Personal Data is:

4.1.1 information concerning child protection matters;

4.1.2 information about serious or confidential medical conditions and information about special educational needs;

4.1.3 information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);

4.1.4 financial information (for example about parents and staff);

4.1.5 information about an individual's racial or ethnic origin; and

4.1.6 political opinions;

4.1.7 religious beliefs or other beliefs of a similar nature;

4.1.8 trade union membership;

4.1.9 physical or mental health or condition;

4.1.10 genetic information;

4.1.11 sexual life;

4.1.12 information relating to actual or alleged criminal activity; and

4.1.13 biometric information (e.g. a pupil's fingerprints following a criminal investigation).

4.2 Staff need to be extra careful when handling Critical Personal Data.

5 Minimising the amount of Personal Data that we hold

5.1 Restricting the amount of Personal Data we hold to that which is needed helps keep personal data safe. If you would like guidance on when to delete certain types of information please refer to the Information and Records Retention policy http://www.e-act.org.uk/policies. If you remain unsure you should contact the Data Protection Officer.

6 Using computers and IT

6.1 A lot of data protection breaches happen as a result of basic mistakes being made when using the Trust's IT system. Here are some tips on how to avoid common problems:

6.2 **Lock computer screens:** Your computer screen should be locked when it is not in use, even if you are only away from the computer for a short period of time. To lock your computer screen press Ctrl Alt Delete. If you are not sure how to do this then speak to IT. Some of the Trust's computers are configured to automatically lock if not used for a period of time but do not rely on this – lock your computer every time it is unattended.

6.3 **Be familiar with the Trust's IT:** You should also make sure that you familiarise yourself with any software or hardware that you use. In particular, please make sure that you understand what the software is supposed to be used for and any risks. For example:

6.3.1 if you use a "virtual classroom" which allows you to upload lesson plans and mock exam papers for pupils then you need to be careful that you do not accidently upload anything more confidential;

6.3.2 make sure that you know how to properly use any security features contained in Trust software. For example, some software will allow you to redact documents (i.e. "black out" text so that it cannot be read by the recipient). Make sure that you can use this

software correctly so that the recipient of the document cannot "undo" the redactions; and

6.3.3 you need to be extra careful where you store information containing Critical Personal Data. For example, safeguarding information should not ordinarily be saved on a shared computer drive accessible to all staff. If in doubt, contact the Data Protection Officer.

6.3.4 make maximum use for all communication and collaboration of the Trust's Microsoft 365 environment.

6.4 **Hardware provided by the Trust:** Staff must not use, download or install any software, app, programme, or service without permission from the IT Department. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to the Trust IT systems without permission.

6.5 **Private cloud storage:** You must not use private cloud storage or file sharing accounts to store or share Trust documents. See 6.3.4 above.

6.6 **Portable media devices:** The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed unless those devices are encrypted and have been given to you by the Trust and you have received training on how to use those devices securely. The IT Department will protect any portable media device given to you with encryption.

6.7 **Disposal of Trust IT equipment:** Trust IT equipment (this includes laptops, printers, phones, and DVDs) must always be returned to the IT Department even if you think that it is broken and will no longer work. These will then be destroyed and data removed securely.

7 Passwords

7.1 Passwords should be long, for example, you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else.

7.2 Your password should be difficult to guess, for example, you could base your password on something memorable that no-one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

7.3 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any Academy account.

7.4 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

8 Emails (and faxes)

8.1 When sending emails or faxes you must take care to make sure that the recipients are correct.

8.2 **Emails to multiple recipients:** You must not use the blind copy function (BCC) to achieve this and take great care in setting up and managing email groups. Check with your IT team for ways in communicating to multiple recipients in a secure manner. If the email or fax contains Critical Personal Data then you should ask another member of staff to double check that you have entered the email address / fax number correctly before pressing send. If a fax contains Critical

Personal Data then you must make sure that the intended recipient is standing by the fax machine to receive the fax.

8.3 **Encryption:** Internal and external emails which contain Critical Personal Data should be encrypted. The Trust uses Office 365 which encrypts data including emails whilst at rest and in transit. Office 365 uses several strong encryption protocols and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES).This encryption should be used when sending details of a safeguarding incident to social services. Confidential documents containing Critical Personal Data should be further encrypted by using password protection. If you need to give someone the "password" or "key" to unlock an encrypted email or document then this should be provided via a different means. For example, after emailing the encrypted documents you may wish to call the recipient with the password. If you have any queries about encryption, for example, if you are unsure how or when to use it, please refer to your IT team.

8.4 **Private email addresses:** You must not use a private email address for Trust related work. You must only use your @E-ACT.org.uk address. Please note that this rule applies to contractors and Academy Ambassadorial Group members as well. Trustees will be required to use an E-ACT email address if they are the Chair of the Board or a Committee to correspond on applicable matters with staff members. For the majority of Board matters (being informed about meetings and that packs are available on BoardEffect), trustees are permitted to use personal email addresses which will be held confidentially by the governance team. Should a decision be taken to override this permission then trustees will be informed separately.

9 Paper files

9.1 **Keep under lock and key:** Staff must ensure that papers which contain Personal Data are kept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure but never overnight). Any keys must be kept safe.

9.2 If the papers contain Critical Personal Data then they must be kept in secure cabinets identified for the specified purpose. Information must not be stored in any other location. These should be fire proof and kept in a secure location. They also need to be too heavy to move to minimise the risk of theft. The cabinets are located around each Academy site as set out in the Academy Paper Files Policy for your Academy.

9.3 **Disposal:** Paper records containing Personal Data should be disposed of securely by placing them in confidential waste bins. Personal Data should never be placed in the general waste. Ensure you are aware where these bins are located in your school.

9.4 **Printing:** When printing documents, make sure that you collect everything from the printer straight away, otherwise there is a risk that confidential information might be read or picked up by someone else. If you see anything left by the printer which contains Personal Data then you must hand it in to the Head Teacher, Regional or National Director. If your Academy uses a "follow me" printing system, this should be used to print all documents.

9.5 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed. Staff may be provided with their own personal secure cabinet(s) in which to store papers. However, these personal cabinets should not be used to store documents containing Critical Personal Data. Please see paragraph 9.2 above for details of where Critical Personal Data should be kept.

9.6 **Post:** You also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If you need to send something in the post that is confidential, consider asking your IT team to put in on an encrypted memory stick or arrange for it to be sent by courier or Special Delivery. Whether courier or Special Delivery is most appropriate will depend on the sensitivity of the personal data contained within the documents. If you are unsure about which method of post to use, please speak to the Regional Operations Director.

10 Working off site (e.g. Academy trips and homeworking)

10.1 Staff might need to take Personal Data off the Academy site for various reasons, for example because they are working from home or supervising an Academy trip. This does not breach data protection law if the appropriate safeguards are in place to protect Personal Data.

10.2 For Academy trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it. You must make sure that Personal Data taken off site is returned to the Academy.

10.3 If you are allowed to work from home then check with the Regional Operations Director or Data Protection Officer what additional arrangements are in place. This might involve installing software on your home computer or smartphone, please see section 11 below.

10.4 **Take the minimum with you:** When working away from the Academy you must only take the minimum amount of information with you. For example, a teacher organising a field trip might need to take with her information about pupil medical conditions (for example allergies and medication). If only eight out of a class of twenty pupils are attending the trip, then the teacher should only take the information about the eight pupils.

10.5 **Working on the move:** You must not work on documents containing Personal Data whilst travelling if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see what you are doing). For example, if working on a laptop on a train, you should ensure that no one else can see the laptop screen and you should not leave any device unattended where there is a risk that it might be taken.

10.6 **Paper records:** If you need to take hard copy (i.e. paper) records with you then you should make sure that they are kept secure. For example:

10.6.1 documents should be kept in a locked case. They should also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g. overnight);

10.6.2 if travelling by train you must keep the documents with you at all times and they should not be stored in luggage racks;

10.6.3 if travelling by car, you must keep the documents out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when your car is stopped e.g. at traffic lights;

10.6.4 if you have a choice between leaving documents in a vehicle and taking them with you (e.g. to a meeting) then you should usually take them with you and keep them on your person in a locked case. However, there may be specific circumstances when you consider that it would be safer to leave them in a locked case in the vehicle out of plain sight. The risks of this situation should be reduced by only having the minimum amount of Personal Data with you (please see paragraph 10.4 above).

10.7 **Public Wi-Fi:** You should not use public Wi-Fi to connect to the internet. For example, if you are working in a cafe then you will either need to work offline or use 3G / 4G on your work mobile to tether the device.

10.8 **Using Trust laptops, phones, cameras and other devices:** If you need to book out a Trust device then please contact your IT team

10.9 Critical Personal Data should not be taken off the site in paper format save for specified situations where this is absolutely necessary, for example, where necessary for Academy trips (see 10.4 above).

11 Using personal devices for Academy work

11.1 You may only use your personal device (such as your laptop or smartphone) for Academy work if you have been given permission by the Regional Operations Director.

11.2 Even if you have been given permission to do so, then before using your own device for Academy work you must speak to your IT team so that they can configure your device.

11.3 **Using your own PC or Laptop:** If you receive permission from your Regional IT lead to use your laptop or PC for Academy work, they can help you prepare your device. This means that Personal Data is accessed through the Trust's own network which is far more secure and significantly reduces the risk of a security breach.

11.4 You must not do anything which could prevent any software installed on your computer or device by the Trust from working properly. For example, you must not try and uninstall the software, or save Academy related documents to an area of your device not protected, without permission from the IT Department first.

11.5 **Using your own mobile phone**: use of a personal mobile phone for work activities is strongly discouraged. If you must use a personal mobile, your emails should only be accessed by the Outlook app. If your mobile is lost or stolen, this is a data breach and you should follow the reporting requirements detailed in the data breach policy.

11.6 **Appropriate security measures** should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date.

11.7 **Default passwords**: If you use a personal device for Academy work which came with a default password then this password should be changed immediately. Please see section 7 above for guidance on choosing a strong password.

11.8 **Sending or saving documents to your personal devices:** Documents containing Personal Data (including photographs and videos) should not normally be sent to or saved to personal devices, unless you have been given permission by the IT Department. This is because anything you save to your computer, tablet or mobile phone will not be protected by the Trust's security systems. Furthermore, it is often very difficult to delete something which has been saved to a computer. For example, if you saved an Academy document to your laptop because you wanted to work on it over the weekend, then the document would still be on your computer hard drive even if you deleted it and emptied the recycle bin.

11.9 **Friends and family:** You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything Academy related on your device. For example, you should not share the login details with others and you should log out of your account once you have finished working by restarting your device. You must also make sure

that your devices are not configured in a way that would allow someone else access to Academy related documents and information – if you are unsure about this then please speak to the IT Department.

11.10 **When you stop using your device for Academy work:** If you stop using your device for Academy work, for example:

11.10.1 if you decide that you do not wish to use your device for Academy work; or

11.10.2 if the Academy withdraws permission for you to use your device; or

11.10.3 if you are about to leave the Trust

then, all Academy documents (including Academy emails), and any software applications provided by us for Academy purposes, will be removed from the device.

If this cannot be achieved remotely, you must submit the device to the IT Department for wiping and software removal. You must provide all necessary co-operation and assistance to the IT department in relation to this process.

12 Breach of this policy

12.1 Any breach of this policy will be taken seriously and may result in disciplinary action.

12.2 A member of staff who deliberately or recklessly discloses Personal Data held by the Trust without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

12.3 This policy does not form part of any employee's contract of employment.

12.4 We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by mail or email.

I confirm that I have read and understood the contents of this policy:

Name	.....
Signature	.....
Date	/ / 20….