challenger multi-academy trust

embrace challenge: expect excellence

Kempston Challenger Academy

GDPR

Information Security Policy

Version: CMAT Board approved – June 2018 v4

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 Challenger Multi Academy (the **Trust**) operates Kempston Challenger Academy (the **School**). The Trust is ultimately responsible for how you handle personal information. In this policy, we use the term "Trust" to mean both the School and the Trust.

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. 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; and

1.3.3 Trust Data Breach Policy

1.3.4 Trust Information and Records Retention policy

1.4 This policy applies to all staff (which includes Governors, agency staff, 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 Headteacher / Head of Operations. Questions and concerns about technical support or for assistance with using IT systems should be referred to local IT / Network managers.

2 Be aware

2.1 Information security breaches can happen in a number of different ways. Examples of breaches which have been reported in the news include:

2.1.1 an unencrypted laptop stolen after being left on a train;

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 on a doorstep.

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 manager and your Headteacher / Head of Operations 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 HR Director / 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).

2.4 You must immediately tell the Headteacher / Head of Operations and if you become aware of anything which might mean that there has been a security breach. You must provide your

Headteacher / Head of Operations with all of the information you have. If you cannot get hold of your Headteacher / Head of Operations or it is outside of school hours then please use this emergency contact number (insert telephone number). 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 individual's privacy more robustly please speak to your Headteacher / Head of Operations.

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 Headteacher / Head of Operations know.

4 Critical School 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 School Personal Data** in this policy and in the data protection policy. Critical School 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 speak to your Headteacher / Head of Operations.

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 the "Windows" key followed by the "L" key. If you are not sure how to do this then speak to IT). The Academy's computers are configured to automatically lock if not used for 8 minutes.

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 School Personal Data. For example, safeguarding information should not ordinarily be saved

on a shared computer drive accessible to all staff. If in doubt, speak to your Headteacher / Head of Operations

6.4 **Hardware and software not provided by the Trust:** Staff must not use, download or install any software, app, programme, or service without permission from the Headteacher / Head of Operations. 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.

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 have been given to you by the Trust and you have received training on how to use those devices securely.

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.

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 school 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:** If an internal email (i.e. only sent to Trust personnel, take care not to copy in unnecessary recipients. All external emails (i.e. to email addresses of people who are **NOT** Trust personnel) to multiple recipients should be double checked by a colleague before these are sent.

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

8.4 **Encryption:** Remember to encrypt internal and external emails which contain Critical School Personal Data. For example, encryption should be used when sending details of a safeguarding incident to social services. To use encryption speak to IT who will explain how to do this. 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.

8.5 **Private email addresses:** You must not use a private email address for Trust related work. You must only use your school or Trust email address. Please note that this rule applies to Governors / Board members as well.

8.6 **Protective Marking of Emails**

The national Protective Marking Scheme sets out five levels of Protective Marking that can be applied to the information we handle to indicate the degree of sensitivity involved. These are used by central Government departments, the emergency services etc. They are: -

1. NOT PROTECTIVELY MARKED (unclassified)
2. RESTRICTED
3. CONFIDENTIAL
4. SECRET
5. TOP SECRET

Local authorities have jointly amended these classifications to reflect the generally lesser impact of the information we use. Our classifications are:

1) UNCLASSIFIED
2) PROTECTED
3) RESTRICTED

The originator of the Email is responsible for deciding the appropriate classification to be applied. You are not considering the likelihood of such a disclosure, just the impact of it. The classification must be decided on. The information should only be given to or shared with people who have a legitimate need to see it as part of their role.

PROTECTED – must be used where the compromise of information would be likely to affect an individual in an adverse manner.

RESTRICTED - is an aggregate effect of the compromise of protected information and data. For example, if a number of files individually marked protected are stored in a database, then the aggregate affect of holding the information together may increase the classification to restricted data.

To clarify, RESTRICTED information is:

- Information that links an identifiable individual with information that, if disclosed, would put them at significant risk of harm or distress OR
- Alternatively any source of information relating to 1000 or more individuals that is not in the public domain, even if the information is not likely to cause harm or distress.

Some examples of data which may affect your classification may include:

- Bank details
- Child Protection/Safeguarding Matters
- SEND Information
- Data containing contact details of children/families/staff
- Credit card numbers
- Contact details
- Benefit details
- Insurance number

The indication of 'Not Protectively Marked' simply provides a positive indication that the information within the Email is not protected or restricted and is therefore unclassified.

If you are unsure about protective marking of information, or you think you have information that you consider may be a higher level than 'RESTRICTED', you should contact your Headteacher or Head of Operations.

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). 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 as set out in the table below. Information must not be stored in any other location, (for example, child protection information should only be stored in the cabinet in the Designated Safeguarding Lead's (**DSL**) room).

9.3 **Disposal:** Paper records containing Personal Data should be disposed of securely. Personal Data should never be placed in the general waste.

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 Headteacher / Head of Operations.

9.5 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed.

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.

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

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

10.2 For School 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 School.

10.3 If you are working from home then you must comply with the remote access agreement (or equivalent) for your school or for the Trust.

10.4 **Take the minimum with you:** When working away from the School 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 must 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.]

10.8 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 school trips (see 10.4 above).

11 Using personal devices for School work

11.1 You may only use your personal device (such as your laptop or smartphone) for School work if you have been given permission by the Headteacher / Head of Operations.

11.2 Even if you have been given permission to do so, then before using your own device for School 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 use your laptop or PC for School work then you must use the remote access software provided by the Trust. Using 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 **Using your own smartphone or handheld:** You should not use your own smartphone or handheld for School work.

11.5 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 School related documents to an area of your device not protected, without permission from the IT Department first.

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 school 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 Headteacher / Head of Operations. 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 a School 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 school 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 School related documents and information.

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

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

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

11.10.3 if you are about to leave the Trust then,

all School documents (including School emails), and any software applications provided by us for School purposes, must 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.