challenger multi-academy trust

embrace challenge: expect excellence

Daubeney Academy

Information Security Policy

	July 2020

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**) 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 must 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 must 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 the information security policy; and

1.3.3 IT acceptable use policy for staff.

1.4 This policy applies to all staff working in the Trust (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes Governors, employees, agency staff, contractors, work experience students and volunteers).

1.5 Any questions or concerns about your obligations under this policy must be referred to the Data Protection Officer. Questions and concerns about technical support or for assistance with using the Trust IT systems must be referred to the IT Department.

2 Be aware

2.1 Information security breaches can happen in a number of different ways. Examples 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 the Data Protection Officer 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 must 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 confidential documents are sometimes left in unlocked rooms at weekends).

2.4 You must immediately tell the Data Protection Officer and the IT Department if you become aware of anything which might mean that there has been a security incident or data breach. This could be anything which puts Personal Data at risk, for example, if Personal Data has been or is at risk of being destroyed, altered, disclosed or accessed without authorisation, lost or stolen. You must provide your manager or the Data Protection Officer with all of the information you have. You must report even if you are not certain that something has gone wrong. For example, if you accidentally send an email to the wrong recipient, or you cannot find some

papers which contain Personal Data. You must report this even if there is no evidence that they have been accessed or stolen.

2.5 In certain situations the Trust must report certain data breaches to the Information Commissioner's Office (the data protection regulator) within 72 hours and let those whose information has been compromised know within strict timescales as well. 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. Personal Data is virtually anything recorded about someone, even something as simple as a person's address or hobbies. If you have any suggestions for how the Trust could improve its data protection / information security practices or protect individual's privacy more robustly please speak to the Data Protection Officer.

3.2 In some situations, 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 which represents a particular risk to an individual's privacy.

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 the Data Protection Officer 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.

4.2 Critical School Personal Data is information which concerns:

4.2.1 safeguarding or child protection matters;

4.2.2 serious or confidential medical conditions;

4.2.3 special educational needs;

4.2.4 financial information including parent and staff bank details;

4.2.5 an individual's racial or ethnic origin; and

4.2.6 political opinions;

4.2.7 religious beliefs or other beliefs of a similar nature;

4.2.8 trade union membership;

4.2.9 someone's physical or mental health or condition;

4.2.10 genetic information;

4.2.11 sex life including sexual orientation;

4.2.12 actual or alleged criminal activity;

4.2.13 allegations made against an individual (whether or not the allegations amount to a criminal offence and whether or not the allegations have been proved; and

4.2.14 biometrics (e.g. if the Trust uses a fingerprint scanner for allowing access to buildings).

4.3 Staff need to be extra careful when handling Critical School 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 but you must never delete Personal Data unless you are sure you are allowed to do so. If you would like guidance on when to delete certain types of information please speak to 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 must be locked when it is not in use, even if you are only away from the computer for a short period of time. If you are not sure how to do this then speak to IT. The Trust's computers are configured to automatically lock if not used for a period of time.

6.3 **Be familiar with the Trust's IT:** You must 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 must not be saved using alumni database software. If in doubt, speak to the Data Protection Officer.

6.4 Specific guidance on the information security requirements of the different programmes that the Trust uses can be obtained from the IT department.

6.5 **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 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.

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

6.7 **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. The IT Department will protect any portable media device given to you with encryption.

6.8 **Trust IT equipment:** If you are given Trust IT equipment to use (this includes laptops, printers, phones, and DVDs), you must make sure that this is recorded on the Trust's IT equipment asset register. School IT equipment must always be returned to the IT Department even if you think that it is broken and will no longer work and the IT equipment asset register updated accordingly.

6.9 **Where to store electronic documents and information:** You must ensure that you only save or store electronic information and documents in the correct location on the Trust's systems. Please ask the IT department for further information.

7 Passwords

7.1 Passwords must be as long as possible and difficult to guess. Do not use single dictionary words. Instead use a passphrase which you create by stringing some words and / or numbers together. Make sure this phrase is memorable but don't choose words or numbers that are linked to you like the names of your family members. Do not choose a password which is so complex that it's difficult to remember without writing it down.

7.2 You must not use a password which you use for another account. For example, you must not use your password for your private email address or online shopping account for any school account. This is because if your personal account is compromised this presents a risk of access to the Trust's systems as well.

7.3 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 must not be written down.

7.4 Sometimes a computer or web browser will allow you to save the password so that you do not need to type it in again next time. You must make sure this does not happen. Pupils can also pose a risk to the School, particularly those pupils who have a good understanding of IT. Many schools have had their computer systems compromised by pupils. If you have any suspicions please raise these.

8 Cyber security and related risks

8.1 Trusts are frequently targeted by attackers looking to take advantage of vulnerabilities in school systems and processes. Sometimes, such attacks will look to exploit technical weaknesses whilst on other occasions, attacks will focus on the human element. For example, they might encourage someone to click on a link in an email by making the email appear as if it has come from a trusted source such as a colleague.

8.2 The following are examples of the types of things to look out for:

8.2.1 a request for information, especially financial information;

8.2.2 a request to click a link or open an attachment;

8.2.3 the sender telling you that it is urgent;

8.2.4 poor language and spelling;

8.2.5 a payment request from a supplier using an email address that is not their usual email address;

8.2.6 unusual sender details or an email address that doesn't look quite right. Often someone may try to pretend that they are emailing you from a School email address. For example, the email address after the @ symbol might contain the name of your school

but the spelling is incorrect or the suffix at the end of the email might be different i.e. not .com or .co.uk.

8.3 Alternatively, an email may appear as if it's from someone who is providing technical support. For example, if might ask for your password or other credentials.

8.4 If you find that you cannot access a particular programme, system or set of data, you must contact your IT team immediately. Whilst this could just be a technical fault, it could be evidence that someone has been able to gain access to the Trust's systems.

8.5 Sometimes the attacker may be someone known to the Trust, such as a parent or pupil. For example, following an acrimonious divorce a parent may set up an email address using the other parent's name in order to try to trick the Trust into sending them information concerning the other parent.

8.6 If you are asked to provide personal data over the phone make sure that the request is genuine. For example, by calling the individual back using the number you have on the system. This must be done even if the person says that they are in a position of authority, such as the police.

8.7 Sometimes hackers create fake advertisements which are displayed on websites. When you click on the advert a malicious programme is downloaded.

8.8 You must also be on your guard if anyone asks you to change Personal Data held by the Trust. Compromising the accuracy of Personal Data is also a breach, even if it is accidental.

8.9 If you have any suspicions or concerns immediately tell the Data Protection Officer and the IT Department.

9 Email, fax and telephone

9.1 You must take care to make sure that the recipients are correct. Getting an email address, fax or telephone number wrong is one of the most common causes of a breach.

9.2 Double check email attachments before sending.

9.3 **Emails to multiple recipients:** If you are sending an email to multiple recipients, you may need to ensure recipient's email addresses are hidden (for example, if emailing multiple parents). This can be done by using a communication platform such as ParentMail or using the "bcc" function. For further details please contact the IT department. It is not always necessary to hide email addresses. For example, when sending a routine email to staff about a timetable change.

9.4 If a fax contains Critical School Personal Data then you must ask another member of staff to double check that you have entered the 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.

9.5 **Encryption:** Remember to encrypt internal and external emails which contain Critical School Personal Data. For example, encryption must be used when sending details of a safeguarding incident to social services. 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 must be provided via a different means. For example, after emailing the encrypted documents you may wish to call the recipient with the password.

9.6 **Non-school email addresses:** You must not use a private email address for Trust related work. You must only use a school email. Please note that this rule applies to Governors as well. Please speak to the IT Department if you require an email account to be set up for you.

10 Paper files

10.1 **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. If you take Personal Data with you to a meeting make sure that you collect all of your papers when you leave.

10.2 If the papers contain Critical School Personal Data then they must be kept in secure cabinets identified for the specified purpose as set out in the table below. Information held in paper format must not be stored in any other location, for example, child protection information must only be stored in the cabinet in the Designated Safeguarding Lead's (**DSL**) room. These [are special cabinets used by the Trust which are fire proof and are kept in a secure location. They are also too heavy to move to minimise the risk of theft. The cabinets are located around the School sites as follows:

Cabinet	Access
[• Child protection - located in the DSL's office]	**[• For each cabinet, set out the procedure for access, who has the key, (there should be at least two people so it can always be accessed in an emergency).]**
[• Financial information]	**[• Ditto]**
[• Health information etc]	**[• Ditto]**

10.3 **Disposal:** Paper records containing Personal Data must be disposed of securely [• by placing them in confidential waste bins which are located [• TBC]]. Personal Data must never be placed in the general waste.

10.4 **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.

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

10.6 **Displays:** Be aware of what Personal Data is on display when the classroom is being used for lessons. For example, would it be possible for pupils to read information that is on your desk while you are teaching?

10.7 **Post:** You also need to be extra careful when sending items in the post. Confidential materials, including anything which contains Critical School Personal Data, must 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.

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

11.1 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.

11.2 For School trips, the trip organiser is responsible for deciding what information needs to be taken and who will look after it. You must make sure that Personal Data taken off site is returned to the School.

11.3 If you are allowed to work from home then check with the IT department what additional arrangements are in place. This might involve installing software on your home computer or smartphone, please see section 12 below. You must never email work containing personal data to your personal email address.

11.4 Not all staff are allowed to work from home. If in doubt, speak to the Data Protection Officer.

11.5 **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 must only take the information about the eight pupils.

11.6 **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 must ensure that no one else can see the laptop screen and you must not leave any device unattended where there is a risk that it might be taken.

11.7 **Return the documents:** Make sure that documents are returned to school. For example, if you print off some information for a school trip, make sure the print out is returned to school.

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

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

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

11.8.3 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;

11.8.4 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 10.5 above).

11.9 **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 4G.]

11.10 **Using Trust laptops, phones, cameras and other devices:** If you need to book out a Trust device then [• describe process].

11.11 Critical School Personal Data must 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 11.5 above).

12 Using personal devices for School work

12.1 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. Please also see paragraph 6.8 above.

12.2 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.

12.3 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.

12.4 **Appropriate security measures** must always be taken. This includes making sure that the firewall on your device is enabled and using anti-virus software. Any software or operating system on your device must be kept up to date by promptly installing updates when they become available. You must make sure that you are using an operating system which is still supported (so you mustn't use an old version of Windows, such as Windows XP, for example).

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

12.6 **Sending or saving documents to your personal devices:** Documents containing Personal Data (including photographs and videos) must not 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 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.

12.7 **Friends and family:** You must not share School Personal Data with your friends and family. For example, you must not share the login details with others and you must 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 – if you are unsure about this then please speak to the IT Department. Disclosing School Personal Data to your friends and family is a data breach, and if you do so knowingly or recklessly, it will also be a criminal offence. The Trust is likely to consider breaches of confidentiality as a disciplinary matter.

12.8 **Social media:** You must never upload or publish Trust information using your personal social media account, even if your account is set to private. For example, you must not upload photographs of pupils under any circumstances.

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

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

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

12.9.3 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, 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.

13 Breach of this policy

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

13.2 A member of staff who deliberately or recklessly obtains or 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. Further information on this and on other offences can be found in the Trust's data protection policy.

13.3 Employees only: This policy does not form part of any employee's contract of employment and may be amended by the Trust at any time.

13.4 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	