Information Security Policy

Adopted with effect from: 25th May 2018

Review date: September 2019

Contents

1 Introduction

1.1 Information security is about what you and Aurora 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 Aurora Academies Trust (**Aurora**) operates City Academy Whitehawk, Glenleigh Park Primary Academy, King Offa Primary Academy, Heron Park Primary Academy, Oakwood Primary Academy and The Gatwick School (the **Schools**). Aurora also employs staff who are not based in schools such as keyworkers. Aurora is ultimately responsible for how you handle personal information. In this policy, we use the term "Aurora" to include both the Schools and the trust itself.

1.3 This policy should be read alongside Aurora's Data Protection Policy which gives an overview of your and Aurora's obligations around data protection. Aurora's Data Protection Policy can be found on the Schools' websites. In addition to the data protection policy, you should also read the following which are relevant to data protection:

1.3.1 Aurora's privacy notices for staff, pupils, parents and families; and

1.3.2 Employment Manual including IT acceptable use policy and .

1.4 This policy applies to all staff (which includes trustees, members of the Local Academy Boards, agency staff, contractors, work experience students and volunteers) when handling Personal Data. For more information on what Personal Data is, please see Aurora's Data Protection Policy.

1.5 Any questions or concerns about your obligations under this policy should be referred to Aurora's Data Protection Officer. Questions and concerns about technical support or for assistance with using Aurora IT systems should be referred to your school's IT support service.

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 School and what you can do to manage the risks. For example, you may wish to develop a checklist to help ensure data protection compliance. Speak to your headteacher or Aurora's Data Protection Officer if you have any ideas or suggestions about improving practices in your School.

2.3 You should immediately report all security incidents, breaches and weaknesses to your headteacher or head of school and Aurora's Data Protection Officer. This includes anything which you become aware of even if you are not directly involved (for example, if you know that offices or filing cabinets are sometimes left unlocked at weekends).

2.4 You must <u>immediately</u> tell your headteacher and Aurora's Data Protection Officer if you become aware of anything which might mean that there has been a security breach. You must provide your headteacher and Aurora's Data Protection Officer with all of the information you have. 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, such as pupil, parent or staff names and/or addresses; 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, Aurora 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 Aurora could protect individual's privacy more robustly please speak to Aurora's Data Protection Officer.

3.2 From May 2018, Aurora 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 Aurora to identify the measures needed to prevent information security breaches from taking place. If you think that such an assessment is required please let Aurora's Data Protection Officer know.

4 Special Category 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 **Special Category Personal Data** in this policy and in the Data Protection Policy. Special Category 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. fingerprints used for controlling access to a building).

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

5 Minimising the amount of Personal Data that we hold

5.1 Restricting the amount of Personal Data that we collect and hold to that which is needed helps keep personal data safe. Please refer to Aurora's Data Destruction Policy for further information.

6 Using computers and IT

6.1 A lot of data protection breaches happen as a result of basic mistakes being made when using Aurora's IT system. It is every member of staff's responsibility to ensure that IT is used correctly. Here are some tips on how to avoid common problems:

6.1.1 **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. To lock your screen press the "Windows" key followed by the "L" key. If you are not sure how to do this then speak to your School's IT support service.

6.1.2 **Be familiar with Aurora'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 if you use a shared drive or virtual classroom you need to be careful that you do not accidently upload anything confidential which may be visible to members of staff or pupils;

6.2 You need to be extra careful where you store information containing Special Category Personal Data. For example, safeguarding or medical information should not ordinarily be saved on a shared computer drive accessible to all staff. If in doubt, speak to your headteacher or Aurora's Data Protection Officer.

6.3 **Hardware and software not provided by Aurora:** Staff must not use, download or install any software, app, programme, or service on hardware owned by Aurora without permission from the headteacher. Headteacher should seek advice from the School's IT support service if required. Staff must not connect (whether physically or by using another method such as wi-fi or Bluetooth) any device or hardware to Aurora IT systems without permission.

6.4 **Private cloud storage:** You must not use private cloud storage or file sharing accounts such as Dropbox or Google Docs to store or share Trust documents.

6.5 **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 Aurora and you have received training on how to use those devices securely. These devices remain the property of Aurora and must be returned upon request.

6.6 **Disposal of Trust IT equipment:** Trust IT equipment (this includes laptops, printers, phones, and DVDs) must always be returned to your School 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 it is your responsibility to make sure that the recipients are correct.

8.2 When forwarding emails you must ensure that all the information contained in the chain of emails is appropriate to share, for example, you must not forward emails containing Personal Data (such as names or emails addresses) unless necessary.

8.3 You may wish to consider anonymising any Personal Data that you send by email, for example by using initials or a pseudonym instead of a real name. You must ensure that the subject is not identifiable from any other information contained in the email.

8.4 **Emails to internal recipients:** Personal Data may be sent by email to internal email addresses but you must only share Personal Data with colleagues where necessary. Please note that City Academy Whitehawk currently use a different email system to other schools in Aurora so emails to/from City Academy Whitehawk should be treated as external emails.

8.5 **Emails to external recipients:** You must think carefully before sending Personal Data by email to external recipients due to the risk of the data falling into the wrong hands. It is recommended that emails to external recipients containing Personal Data are encrypted or password protected (see 8.7 below). This includes emails sent to City Academy Whitehawk email addresses from a non-City Academy Whitehawk email address.

8.6 **Emails to multiple recipients**: When sending emails to multiple recipients all recipients will be able to see the emails addresses placed in the "To:" address line. Therefore you must ensure that you have permission to share these email addresses. If you do not have permission, you must place their email address in the "Bcc:" address line so their email address is not visible to other recipients.

8.7 If the email or fax contains Special Category Personal Data or if you are sending large amounts of Personal Data (for example in a spreadsheet or a report) 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 Special Category Personal Data then you must make sure that the intended recipient is standing by the fax machine to receive the fax.

8.8 **Encryption:** When sending Personal Data to external recipients it is recommended that you encrypt the email or use password protection (see below). All external emails which contain Special Category Personal Data must be encrypted. For example, encryption must be used when sending details of a safeguarding incident to social services. To use encryption then you need speak to your headteacher or IT support service 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.

8.9 **Protecting documents with a password**: Files created in Microsoft Office can be protected by setting a password. To set a password on your Word, Excel or PowerPoint file click File > Info > Protect Document > Encrypt with Password. You'll be prompted to create a password, then to confirm it. After you've added a password to your file save the file to make sure the password takes effect. When sending a password protected file, you must provide the password to the recipient via a different means. For example, after emailing the encrypted documents you may wish to call the recipient with the password.

8.10 **Private email addresses:** You must not use a private email address for any Aurora related work or communications. You must only use your school address. Please note that this rule applies to trustees and Local Academy Board members. Please speak to your School office if you require an email account to be set up for you.

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 Special Category 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 designated cabinet. These special cabinets used by Aurora which are fire proof and are kept in a secure location. They are also too heavy to move to minimise the risk of theft.

9.3 **Disposal:** Paper records containing Personal Data should be disposed of securely by placing them in the School's confidential waste bins. Personal Data must 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 or Aurora's Data Protection Officer.

9.5 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed. Special Category Personal Data must be kept in the designated cabinet and not in a personal locker or desk.

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 using an encrypted memory stick or arrange for it to be sent by courier.

10 Medical information

10.1 Schools may need to display medical information about pupils to ensure staff act appropriately in case of an emergency. Medical information may also be passed to catering staff to inform them of any pupils with allergies.

10.2 Only necessary information should be displayed, for example pupil name, photograph and essential medical history. Information must not be displayed where it may be visible to visitors. Information must be updated regularly and must be removed when no longer relevant.

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 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.

11.3 If you have permission to work from home then check with your headteacher or Aurora's Data Protection Officer what arrangements are in place to allow you to do this securely. This might involve installing software on your home computer or smartphone, please see section 12 below.

11.4 **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 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.

11.5 **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.

11.6 **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:

11.6.1 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);

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

11.6.3 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;

11.6.4 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 11.4 above).

11.7 **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.

11.8 **Using Trust laptops, phones, cameras and other devices:** Your School may have devices that you can borrow for working off site. Please speak to your headteacher for more information.

11.9 Special Category 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 11.4 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 your Headteacher.

12.2 **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 Aurora or access documents via Office 365. This means that Personal Data is accessed through Aurora's own network which is far more secure and significantly reduces the risk of a security breach.

12.3 **Using your own smartphone or handheld:** Aurora reserves the right to monitor, review and erase, without further notice, all content on the device that has been created for Aurora or on Aurora's behalf or which contains Personal Data. This includes all emails sent and received via your School email account. Although we do not intend to wipe other data that is private in nature (such as private photographs or private files or emails), it may not be possible to distinguish all such information from Personal Data in all circumstances. You should therefore regularly back up any private data contained on the device or keep private material separate via a partition that would not be remotely wiped in these circumstances.

12.4 You must not do anything which could prevent any software installed on your computer or device by Aurora 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.

12.5 **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 must be kept up to date.

12.6 **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.

12.7 **Sending or saving documents to your personal devices:** Documents containing Personal Data (including photographs and videos) must never be sent to or saved to personal devices. This is because anything you save to your computer, tablet or mobile phone will not be protected by Aurora'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.

12.8 **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 – if you are unsure about this then please speak to your School's IT support service.

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 Aurora

then, all School documents (including 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 School's IT support service for wiping and software removal. You must provide all necessary co-operation and assistance to the School and its IT support service 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 discloses Personal Data held by Aurora without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

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

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	