INFORMATION SECURITY POLICY

The OHC&AT Board of Trustees has agreed this Policy – 1st July 2022.

Jay Mercer
Chair of OHCAT Board

Peter Lauener
Chair of OHC Board

Information Security Policy

1. INTRODUCTION

Information security is about what you and OHC&AT need to do to help make sure that **personal data** is kept safe. This is the most important area of data protection to get right. Most data protection fines have come about because of information security breaches.

This policy must be read alongside OHC&AT's Data Protection Policy – Practical Guidance for Staff, which gives an overview of your and OHC&AT's obligations around data protection. OHC&AT's data protection policy can be found on the website and intranet. In addition to this policy and the Data Protection Policy, you must also read the following which are relevant to data protection:

- OHC&AT's privacy notices for pupils/students, parents/carers and staff
- IT Acceptable Use Policy
- Guidance for Staff on the Use of Photos and Videos
- Data Breach Policy

This policy applies to all staff working in OHC&AT (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities; this includes employees, Trustees, Governors, contractors, agency staff, work experience/ placement, students and volunteers.

Data protection is the responsibility of everyone in OHC&AT, and it is important that you read and understand the relevant policies so that you know what you should do day-to-day, but also what to do when something goes wrong.

Any questions or concerns about your obligations under this policy must be referred to the Data Protection Officer, GDPR Sentry Limited, Unit 434 Birch Park, Thorp Arch Estate, Wetherby, LS23 7FG, 0113 804 2035 or via the Business Support Partner (Rachael Tucker), data.protection@ohcat.org, 020 3897 7002. Questions and concerns about technical support or for assistance with using OHC&AT IT systems must be referred to the IT Department.

Employees only: This policy does not form part of your contract of employment and may be amended by OHC&AT at any time.

OHC&AT reserves the right to change this policy at any time. Where appropriate, we will notify staff of those changes by mail or email.

2. BE AWARE

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

- opening a suspicious attachment on an email;
- not being able to access the only copy of a document because the password has been forgotten;

- a stolen or lost laptop or device;
- personal data held to ransom following a website hack;
- sending a confidential email to the wrong recipient;
- leaving documents containing personal data in an unsecure or public area.

These should give you a good idea of the sorts of things which can go wrong, but please think about problems that 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 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.

If you become aware of anything which might mean that there has been a security incident or data breach, or if you become aware of a practice that weakens the OHC&AT's defences in relation to the protection of personal data, you must immediately tell your line manager who will advise you how to inform the Data Protection Officer and/or the IT Department. 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. Another example might be where you become aware that a particular department has developed a habit of leaving confidential documents in unlocked classrooms.

You must provide 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.

In certain situations OHC&AT must report 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.

You should report even if you are not directly involved.

3. THINKING ABOUT PRIVACY ON A DAY TO DAY BASIS

You should be thinking about data protection and privacy whenever you 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 OHC&AT could improve its data protection/information security practices or protect individual's privacy more robustly please speak to the Data Protection Officer.

In some situations, OHC&AT is required to carry out an assessment of the privacy implications of using personal data in certain ways, e.g. when we introduce new technology which represents a particular risk to an individual's privacy. These assessments are known as data protection impact assessments (DPIA).

These assessments help OHC&AT to identify the measures needed to prevent information security breaches from taking place. If you think that such an assessment is required or would be helpful, please let the Data Protection Officer know.

4. CRITICAL OHC&AT PERSONAL DATA

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

Critical OHC&AT Personal Data is information which concerns:

- safeguarding or child protection matters;
- serious or confidential medical conditions;
- special educational needs;
- financial information including parent/carer or staff bank details;
- an individual's:
    - racial or ethnic origin;
    - political opinions;
    - religious beliefs or other beliefs of a similar nature;
    - trade union membership;
    - physical or mental health or condition;
    - sex life including sexual orientation;
- actual or alleged criminal activity;
- serious allegations made against an individual (whether or not the allegations amount to a criminal offence and whether or not the allegations have been proved);
- biometrics (for example if an academy uses a fingerprint scanner for allowing access to buildings); and
- genetic information.

Staff need to be extra careful when handling Critical OHC&AT Personal Data.

5. MINIMISING THE AMOUNT OF PERSONAL DATA THAT WE HOLD

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 refer to the Information and Records Retention Policy which can be found on the staff intranet or speak to the Data Protection Officer.

6. USING COMPUTERS AND IT

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

- **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 computer screen press and hold the "Windows" key followed by the "L" key, or hold down the “Ctrl”, “Alt” and “Delete” keys simultaneously to bring up the lock screen menu. If you are not sure how to do this then speak to

IT. As a fail-safe OHC&AT's computers are configured to automatically lock if not used for 10 minutes but this does not apply to classroom PCs and staff must lock or close down classroom PCs when they are not in use.

- **Be familiar with OHC&AT'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:
    - 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;
    - make sure that you know how to properly use any security features contained in OHC&AT 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
    - you need to be extra careful where you store information containing Critical OHC&AT Personal Data. For example, safeguarding information must not be saved in a public location. If in doubt, speak to your line manager or the Data Protection Officer.
- **Hardware and software not provided by OHC&AT:** Staff must not use, download or install any software, app, programme, or service without permission from the IT team. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to OHC&AT IT systems without permission.
- **Private cloud storage:** You must not use private cloud storage or file sharing accounts to store or share OHC&AT documents. You must only use cloud storage provided by OHC&AT.
- **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 OHC&AT and you have received training on how to use them securely. The IT team will protect any portable media device given to you with encryption. You must not plug in or connect anything not provided by OHC&AT to OHC&AT computers or other equipment, even if it looks harmless. This is because something that looks innocuous such as a USB charging cable can be harmful.
- **OHC&AT IT equipment:** If you are given OHC&AT IT equipment to use (this includes laptops, printers, phones, and DVDs), you must make sure that this is recorded on OHC&AT's Asset Register. OHC&AT IT equipment must always be returned to the IT team even if you think that it is broken and will no longer work, and the Asset Register updated accordingly.
- **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 OHC&AT's systems. Many locations are restricted to certain staff; if you need access to a particular location you should contact the owner to seek permission.

7. PASSWORDS

Passwords must be as long as possible and difficult to guess. Do not use single dictionary words. Instead you can either use a passphrase which you create by

stringing some words and/or numbers together, or you can follow the National Cyber Security Centre guidance on passwords which suggests using three random words.

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.

If you are using the three random words method make sure that the words are unrelated to each other. The advantage of this type of password is that three well-chosen random words can be easy to remember but not easy to guess.

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 OHC&AT account. This is because if your personal account is compromised this presents a risk of access to OHC&AT's systems as well.

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.

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. If a password manager is used you should ensure that there is another login step before anyone could access the account with the saved password (e.g. Windows account login, multi factor authentication).

You must ensure that your password is kept safe and not revealed or divulged to pupils/students, staff or visitors.

If you think that your password has been compromised you must change it immediately to something that is not similar to your previous password.

8. CYBER SECURITY AND RELATED RISKS

Schools and colleges are frequently targeted by attackers looking to take advantage of vulnerabilities in their 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.

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

- a request for information, especially financial information;
- a request to click a link or open an attachment;
- the sender telling you that it is urgent;
- poor language or spelling;
- a payment request from a supplier using an email address that is not their usual email address 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 an OHC&AT 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 .org or .ac.uk.

Alternatively, an email may appear as if it's from someone who is providing technical support. For example, it might ask for your password or other credentials. **Never** share your password with anyone. IT will never ask for this.

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 OHC&AT's systems.

Sometimes the attacker may be someone known to OHC&AT. 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 OHC&AT into sending them information concerning the other parent.

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.

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

You must also be on your guard if anyone asks you to change personal data held by OHC&AT. Compromising the accuracy of personal data is also a breach, even if it is accidental.

If you fall victim to any form of scam or attack, you MUST report this immediately so that OHC&AT can take the necessary steps to minimise the impact of the action, and report where necessary.

The National Cyber Security Centre provides a free service to report suspicious emails at https://www.ncsc.gov.uk/information/report-suspicious-emails

If you have any suspicions or concerns, or need to report a potential attack, tell the IT team immediately.

9. EMAIL, FAX AND TELEPHONE

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.

Double check email attachments before sending.

Emails to multiple recipients: Avoid sending emails to multiple recipients as far as possible. Don’t copy people into emails unless it is information that they absolutely

need to receive. Use the 'reply all' option judiciously, only reply to those who need to receive your reply. Review email trails and delete any unnecessary history from your reply.

Do not send all staff emails; this is only done with permission of the CEO, Deputy CEO or College Principal.

It is not always necessary to hide email addresses by using bcc option. For example, when sending a routine email to staff about a timetable change. Only use the bcc option to protect a recipient's privacy.

If a fax contains Critical OHC&AT 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 OHC&AT Personal Data then you must make sure that the intended recipient is standing by the fax machine to receive the fax.

Encryption: Remember to encrypt internal and external emails which contain Critical OHC&AT Personal Data. For example, encryption must be used when sending details of a safeguarding incident to social services. See Appendix 1 for details on 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.

Non-OHC&AT email addresses: You must not use a private email address for OHC&AT related work. You must only use an OHC&AT email address. Please note that this rule applies to Trustees and Governors as well when sending or receiving personal data. Please speak to the IT team if you require an email account to be set up for you.

10. PAPER FILES

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.

If the papers contain Critical OHC&AT Personal Data then they must be kept in secure cabinets identified for the specified purpose.

Disposal: Paper records containing personal data must be disposed of securely by placing them in confidential waste bins/shredded. Personal data must never be placed in the general waste.

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 to the originator or securely dispose of it.

Put papers away: OHC&AT operates a 'Clean Desk Policy', you must therefore always keep a tidy desk and put papers away when they are no longer needed. Staff are provided with secure cabinet(s) in which to store papers. However, these cabinets must not be used to store documents containing Critical OHC&AT Personal Data.

Displays: Be aware of what personal data is on display; never leave personal data an unsecure or unsupervised area or in a way in which it would be possible for others to read information.

Post: You also need to be extra careful when sending items in the post. Confidential materials, including anything which contains Critical OHC&AT 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 it on an encrypted memory stick or arrange for it to be sent by courier.

11. WORKING OFF SITE (e.g. OHC&AT TRIPS AND HOMEWORKING)

Staff might need to take personal data off OHC&AT sites for various reasons, for example because they are working from home or supervising an educational trip. This does not breach data protection law if the appropriate safeguards are in place to protect personal data.

For OHC&AT trips, the Educational Visit Coordinator 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 secure at all times and returned to OHC&AT.

If you are allowed to work from home then check with your line manager what additional arrangements are in place in relation to paper records and accessing information electronically. You must not connect your personal phone or tablet email software to the OHC&AT email system. If you need a phone to carry out your duties you should speak to your line manager in the first instance. You must never email work containing personal data to your personal email address.

Take the minimum with you: When working away from OHC&AT you must only take the minimum amount of information with you. For example, a teacher organising a field trip might need to take with them information about pupil medical conditions such as 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.

Working on the move: You must not work on documents containing personal data whilst travelling if there is a risk of unauthorised disclosure (e.g. 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.

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

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

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

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.

Using OHC&AT laptops, phones, cameras and other devices: If you need an OHC&AT device then speak to your line manager.

Critical OHC&AT 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 above). Other than for OHC&AT trips, you must obtain authorisation from the Data Protection Officer.

When you finish at OHC&AT: When you leave OHC&AT (e.g. to start a new job or to retire) you must return any personal data (and documents containing personal data) to your line manager before the end of your last day (or earlier if requested). For example, if you have been given permission to keep papers at home you will need to make sure that these are returned. Please also see section 12 below in relation to electronic devices used for OHC&AT work.

12. USING PERSONAL DEVICES FOR OHC&AT WORK

Personal devices should not be used for work unless absolutely unavoidable, and you may only use your personal device (such as your laptop or smartphone) for OHC&AT work if you have been given permission by the IT Manager. Please also see section 6 above.

Even if you have been given permission to do so, then before using your own device for OHC&AT work you must speak to your IT team so you understand how you can use the device for OHC&AT work.

Using your own laptop or PC: If you use your laptop or PC for OHC&AT work then you must use the remote access software provided by OHC&AT (Parallels). Using Parallels means that personal data is accessed through OHC&AT's own network which is far more secure and significantly reduces the risk of a security breach as the

data is encrypted. All links to the remote desktop are on the OHC&AT website via the Remote Access link.

Using your own smartphone or handheld device: You must not use your own smartphone or handheld device for OHC&AT work.

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 7, for example).

Downloading apps and software: You must take care when downloading apps and software onto your personal device if it is used for OHC&AT work. This is the case even if you are using remote access software. Hackers can exploit vulnerabilities in your personal device to access OHC&AT Personal Data. Please only download apps from official app stores like the Apple App Store and Google Play. If you have any questions please speak to the IT Department.

Screen lock and password: You must have a screen lock on any mobile device used to access OHC&AT Personal Data (e.g. a passcode or fingerprint). Any computer (e.g. laptop) used for OHC&AT work must be protected with a strong password (see section 7 above).

Default passwords: If you use a personal device for OHC&AT work which came with a default password, this password must be changed immediately. You must also change the default password on any account used for work reasons even if you are not using it to share Personal Data. Please see section 7 above for guidance on choosing a strong password.

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. This is because anything you save to your personal computer, tablet or mobile phone will not be protected by OHC&AT'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 OHC&AT 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.

Friends and family: You must not share OHC&AT personal data with your friends and family or allow them to access or see OHC&AT personal data. For example, you must not share the login details with others and you must log out of your account once you have finished working and restart your device. You must also make sure that your devices are not configured in a way that would allow someone else access to OHC&AT-related documents and information – if you are unsure about this then please speak to the IT team. Disclosing OHC&AT 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. OHC&AT is likely to consider breaches of confidentiality as a disciplinary matter.

Social media: You must never upload or publish OHC&AT information using your personal social media account, even if your account is set to private. For example, you must not upload photographs of pupils or students under any circumstances. All communication with pupils/students and families must be through OHC&AT systems – it is not acceptable to communicate with pupils/students/families through personal social media channels or other technology based platforms, unless there is a pre-existing relationship that has been declared via your annual Declaration of Interest form. Any communication through social media or any technology based platforms used for interacting or discussion via voice, text, video or pictures must conform to all OHC&AT policies. Staff are strongly advised to ensure that appropriate privacy settings are in place on any and all personal social media accounts, whilst remaining aware that all online interactions are potentially accessible – a useful rule of thumb is to always consider that everyone can and will read everything you write.

When you stop using your device for OHC&AT work: For example:

- if you decide that you do not wish to use your device for OHC&AT work; or
- if OHC&AT withdraws permission for you to use your device; or
- if you are about to leave OHC&AT

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

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

Breach of this policy

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

A member of staff who deliberately or recklessly obtains or discloses personal data held by OHC&AT (or procures its disclosure to another person) 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 OHC&AT's Data Protection Policy.

POLICY REVIEW DETAILS

Version:	1.2
Reviewer:	Rachael Tucker
Approval body:	Family Board
Date this version approved:	1st July 2022
Due for review:	Summer 2023

RELATED POLICIES AND DOCUMENTATION

Child Protection Adult Protection and Safeguarding Policy
Data Protection Policy
Information and Records Retention Policy

IT Acceptable Use Policy
Personal Data Breach Policy and Procedure
Social Media Policy
Staff Code of Conduct

Appendix 1: Options for sending or receiving secure email

You must use one of the following 3 options when sending OHC&AT **Critical Data** by email internally or externally.

1. **Encrypt.** Adding the word “encrypt” anywhere in the title bar of the email will encrypt the email and any attachment. The receiver will need to either confirm their own Microsoft account password or use a one-time passcode before they can open the email and any attachments.
2. **Egress**. Egress is web-based software for sending and receiving encrypted email and attachments. It is used by many Local Authorities and government departments. It is free to reply to an email received by Egress or to send a message via Egress if the recipient has a paid for Egress account. You can also send up to 25 emails (25 credits) by Egress if neither you nor the receiver are paid users. See the attached for more details on how to set up a free Egress account.
3. **Password Protect**. You can encrypt a file with a password. The procedure to set a password for any Microsoft office file is:
   - Open the Microsoft Office file you want to protect
   - Click File
   - Click Info
   - Click Protect Document
   - Click Encrypt with Password
   - Enter a password to restrict opening the document or modifying it or both and click OK
   - Confirm your password and click OK

   You can add a password to a Microsoft office document when you save it as a PDF:
   - Click File
   - Click save as
   - Click save as type – PDF
   - Click Options
   - Encrypt the document with a password etc. …..

   but you will not be able to add a password to an existing PDF file unless you have Adobe Acrobat Pro DC.

Appendix 2: Information Security Essentials

These are the key points to remember about information security. You must still read and follow the Information Security Policy but this is a quick overview of some of the key points.

1. Speak to the Head of Business Compliance (rtucker@orchardhill.ac.uk, 07792 105409) if you have any concerns, questions or suspicions.

2. If you have any questions about OHC&AT's IT systems speak to the IT Department.

3. If it's an emergency (e.g. you suspect a data breach) call Rachael Tucker 07792 105409 or Lynn Barratt

4. If you need to dispose of any OHC&AT Personal Data this must be done securely (e.g. use confidential waste bins for paper).

5. Your passwords must be strong and unique (please see section 7 of the Information Security Policy for more information).

6. OHC&AT Personal Data must never be sent to a non-school email account.

7. Be on your guard for suspicious emails, texts and phone calls. Never click on a link, open an attachment or provide information if you have any doubts - check with the IT Department first. See section 8 of the Information Security Policy.

8. Be extra careful to keep Personal Data secure when working away from the OHC&AT sites. For example, only take the minimum amount of Personal Data with you. See section 11 of the Information Security Policy.

9. You must only use a personal device (e.g. phone, tablet, laptop) for school work if this has been approved by your line manager and you understand how to access OHC&AT Personal Data securely. See section 12 of the Information Security Policy.

10. Personal Data must be sent securely. Never send anything confidential or sensitive by normal post. See appendix I if you need to send something electronic securely.