



2022

# 1 to 1 Digital Learning Program

## **School vision**

East Doncaster Secondary College aims to develop independent and interdependent, reflective, global learners who strive to improve in learning and achieve our best. This includes developing the confidence to take risks, trusting self and others, using initiative and being able to adapt to change or to emerging needs and trends. We value learning with and from others, developing teams of enquiring people, encouraging meaningful conversations and valuing the contributions of others. At the same time we want to be outward looking, searching for greater knowledge and inviting others to support us in establishing a culture of curiosity.

The 1 to 1 Digital Learning Program will support us to continue the provision of the highest quality education to our school community. The effective use of ICT helps to engage students in their learning and assists in individualising student programs. It also assists students in making connections with what they are learning and with the world outside of the classroom. Tools and processes for effective communication, collaboration and creating collective meaning between teachers, students, parents and the school community is additionally enhanced through our 1 to 1 program. Improved access to computers will provide a platform for deeper understanding of concepts and information for all students at all times. It will give teachers consistent access to tasks that are whole-world, big picture, instantly.

East Doncaster Secondary College continues its whole school 1 to 1 Digital Learning Program. That is, one learning device for each individual student. The College supports a range of devices that support our minimum requirements, including Windows and macOS devices.

## **Program overview**

East Doncaster Secondary College gives families the choice to purchase a device that meets our minimum specifications. This way, families have the choice to purchase a device through a reseller of their choice. The College recognises that having a single device model does not always meet the requirements or preferences of every student and their family.

The College has minimum specifications that devices must meet in order for the device to fully integrate with our IT and AV services. These requirements allow for a range of hardware and software.

## **Device ownership**

It is important to note that the storage capacity of all devices is for required licensed software and students' work files. If there is some excess capacity other files may be held in storage.

Nevertheless school software and files must remain priority and be available at all times without exception.

The College reserves the right to delete inappropriate programs or material and to disconnect the device from the College network for a period of time if it is used inappropriately.

The acceptable use of digital devices is explained in the EDSC Acceptable Use Agreement.

### **Device replacement schedule**

When a student purchases a new device in Year 7, it is anticipated they will keep this until the end of Year 10 and purchase a new device for VCE. Devices over 4 years of age are likely to underperform, be unreliable and potentially impact student learning.

### **Device configuration**

All devices will need to be configured to ensure they can operate on the EDSC network and, where applicable, loaded with all of the software licensed for student use.

### **Optional peripherals**

The school will not provide or specifically recommend any additional peripherals as part of the 1 to 1 Digital Learning Program. However, parents or students may purchase these outside of the program. Program support and warranty will not apply to peripherals.

Peripherals may include:

- Headphones
- Wireless mouse
- HDMI adapter

### **Use of school bags for added security**

An important expectation is that all students will use their EDSC school bag to transport their digital devices to and from school. All students from Years 7-12 are expected to use EDSC school bags as a compulsory part of school uniform. Official EDSC School bags are available from PSW or Reception.

## **Access to school lockers**

All students will be provided an individual locker. Each student is required to provide their own quality lock to secure their property from the first day of attendance at school each year.

## **EDSC Acceptable Use Agreement and program payment**

You are required to read thoroughly through the 'EDSC Acceptable Use Agreement' document. This agreement requires you and your child to agree to use the intranet, internet, digital and mobile technologies responsibly. Access to the EDSC network cannot be granted unless this Agreement has been formally accepted. The 'EDSC Acceptable Use Agreement' document has been provided in the induction pack of all new students to the College.

All students and their parents are required to complete and sign the EDSC Acceptable Use Agreement via Compass.

If you have any questions, please contact Assistant Principal Karen Boyle at the College.

## **Technical support**

General technical support is available for all devices from the Technical Support Team in the Technical Support office (next to room 107).

## **Warranty and repairs**

If a digital device is faulty or damaged it should be taken to the IT Department for a technical assessment. Students will be given advice on the next step for repair and/or warranty claims. Repair and warranty claims are handled by third party companies. A Lenovo or HP device previously purchased through the JB Hi-Fi Solutions portal can be serviced on site by a JB Hi-Fi technician.

## **Insurance**

Parents need to make prior insurance arrangements for the cost of repairs required if a device is dropped or broken.

The College does NOT underwrite insurance costs for damaged digital learning devices. Whilst not compulsory, parents have full responsibility for insuring these devices or paying for any repairs required. Insurance claims will not be processed by EDSC IT Support or the General Office.

## Frequently asked questions

### **1. Who can I contact if I have further questions?**

Questions regarding the Digital Learning Program can be directed initially to the General Office on (03) 9842 2244. Your enquiry will be responded to as quickly as possible.

### **2. Will a student be using their digital learning device in every subject every day?**

A student will not necessarily be required to use the computer at all times. The use of computers will take place alongside a range of learning activities. However the device is an essential learning tool that must be available to be utilised when required and therefore should be taken to all classes unless specifically advised.

### **3. Where will a student store their digital learning device when it is not in use?**

Students must store and secure their device, in their protective case, in their locker during recess and lunch times. If students are unable to secure their device at these times they should report to the appropriate sub-school office. Students will need to store their devices in their lockers before Physical Education practical classes unless otherwise instructed by their class teacher.

### **4. Can a student add their own software to their device?**

Yes, providing the software will not impact other EDSC users negatively. Alternate Anti-Virus products must be installed with caution as they often interfere with network and internet connectivity.

### **5. What is the process if my child exits the school?**

Parent or student owned computers are the property of the family and therefore will be taken with the student, however any DET licensed software must be removed prior to departure. Families will be responsible for any finance agreements pertaining to the device. Devices owned by EDSC must be returned prior to departure.

### **6. Is my child expected to take their device home every day?**

Yes, students are expected to take the device to and from school each day. This will enable them to fully utilise it at home and at school. It is expected that computers will be charged overnight ready for a full day's use at school. Parents are asked to ensure that the computer is used responsibly and cared for appropriately in the home environment. Devices must be transported within their protective cases inside the student's school bag to and from school.

### **7. Can I recharge my computer at school?**

It is expected that a student's computer has a good working battery that has more than six hours charge. The device must be fully charged on arrival at school. Students must be aware that the use of the device outside class time may impact the ability to remain charged for all classes.

### **8. What happens if the battery goes flat?**

Students are required to bring their devices to school fully charged every day.

### **9. Can other people use the device?**

While it is a family owned device, it is required for the student's education, so it is recommended that it is not used by anybody else.

### **10. Can the device be taken overseas?**

Parents are advised to check the insurance provisions they have selected on the device to determine what cover is provided.

### **11. Will the student software on their computer be private?**

Students can expect their computers to be periodically inspected and monitored for inappropriate usage. Students and parents need to be aware that apps stored locally on the device or on school servers are not private.

### **12. What happens if my child leaves their device at home?**

Students will be significantly disadvantaged as they will not be able to borrow computers from the College. It is the responsibility of the student to ensure that they bring their device every day. Continual failure will lead to intervention and consequences as decided upon by the College.

### **13. Does my home need Internet access?**

No. Students will be able to access the information they need when they are at school. Even when not connected to the internet, notebook computers are still very useful tools for learning. Of course, if you have Internet access at home, you are welcome to connect the device to your Internet connection.

### **14. Do I need to buy a new device?**

Year 7 students are expected to start at EDSC with a new device that should last for 4 years and be replaced when starting VCE.

Other year levels are expected to use a device comparable in age or newer.

Devices over 4 years of age are likely to underperform, be unreliable and potentially impact student learning. Older devices will be scrutinised more carefully to determine their suitability prior to enrolment.

#### **15. Can I use one device for six years?**

If parents would like their child/children to use a single device for six years, students must ensure the device is kept in good working order and the battery must be replaceable and replaced at least once in that duration. Failures due to aging hardware will be the responsibility of parents and students. Students must not be dependant on mains power to operate their computer while at EDSC.

#### **16. Can I purchase a gaming device?**

EDSC does not recommend gaming devices due to weight and battery life.

#### **17. Can I use my device for gaming?**

While we recognise that students may want to use their device for other purposes, such as gaming, this will shorten the life of the device and its battery. It is recommended that students who are frequent gamers have a dedicated device for that purpose.

# 1 to 1 Digital Learning Program Summary

## **Program options**

1. Purchase a Windows Laptop or Apple Macbook.  
It is mandatory that the device meets the EDSC requirements (Attachment B).
2. Bring a Windows Laptop or Apple Macbook.  
It is mandatory that the device meets the EDSC requirements (Attachment B).

## **Required accessories**

1. A device bag or slipcase that protects the computer from damage caused by dropping

Choose the option that best suits your needs.

Please refer to the Digital Learning Program Timeline for key dates.



# Attachment A

## Provided support

1. Required Software will be available for download and Install
2. Software and Configuration support will be provided on a best effort basis.
3. Students will retain full right to the computer, allowing for the installation of additional peripherals and software.
4. Warranty claims will be managed by parent/student.
5. Hardware repair not available on-site/campus.
6. Insurance claims will be managed by parent/student.

# Attachment B

## Parent/student selected devices

### Required hardware specifications

Parent or student selected devices are required to adhere to the following guidelines:

- **Device Type:** Laptop, notebook or tablet capable of supporting Microsoft Windows 11, Windows 10 or macOS.
- **Device Age:** A student will purchase a new device in Year 7. It is anticipated they will keep this until the end of Year 10 and purchase a new device for VCE. Devices over 4 years of age are likely to underperform, be unreliable and potentially impact student learning. If parents would like their child/children to use a single device for six years, students must ensure the device is kept in good working order and the battery must be replaceable and replaced at least once in that duration.
- **Storage:** Minimum 128GB. (Recommended: SSD/Flash Storage)
- **Screen Size:** 10.8” to 15.6” (Recommended: 11.6” – 13.3”). While permitted, 15” laptops are not recommended as they are unlikely to meet weight and battery life requirements.
- **Weight:** Under 2kg (Recommended: under 1.6kg)
- **Battery Life:** 6+ hours (During general use, not idle)
- **Input:** Physical Keyboard, attached or detachable
- **Display Ports:** HDMI
- **Other Ports:** 1x USB, 3.5mm Headphone Jack
- **Wireless Network:** Wi-Fi supporting wireless “N”, “AC” or “AX” standard (Recommended: Intel Network Adaptor with “AX” support)
- **Operating System:** Microsoft Windows 11, Microsoft Windows 10 64Bit (English Language Only) or Apple macOS 11, 10.15 (English Language Only)
- **Language:** English Language Only

**Devices that do not meet these requirements are not supported for use at EDSC.**

**Be sure to seek advice before making a purchase.**

**Gaming laptops are not recommended.**

## **Windows 10 S Mode is not supported.**

### **Mandate for VCE creative arts subjects (including VCE Studio Arts, VCE Visual Communications and Design, VCE Media)**

1. Device Type: Laptop, notebook capable of supporting Microsoft Windows 11, Windows 10 or macOS.
2. Processor intel i5 or equivalent
3. Memory: 8Gb minimum (Recommended : 16Gb)
4. Storage: Minimum 256GB SSD/Flash Storage (Recommended: 512Gb)
5. Screen Size : 12” to 15.6”
6. Dedicated graphics card recommended
7. Weight : Under 2kg (Recommended: under 1.6kg)
8. Battery Life : 6+ hours (During general use, not idle)
9. Input : Physical Keyboard/mouse, attached or detachable
10. Display Ports : HDMI
11. Other Ports : 1x USB, 3.5mm Headphone Jack
12. Wireless Network : Wi-Fi supporting wireless “N”, “AC” or “AX” standard (Recommended: Intel Network Adaptor with “AX” support)
13. Operating System: Microsoft Windows 11, Microsoft Windows 10 64Bit (English Language Only) or Apple macOS 11, 10.15 (English Language Only)
14. Accessories: Headphones, multiport USB hub for devices with USB-C (which includes SD card reader and USB-A).

### **Mandate for VCE Information Technology (IT) subjects**

1. Device Type: Laptop, notebook capable of supporting Microsoft Windows 11, Windows 10, Apple devices are not recommended
2. Processor intel i5 or equivalent
3. Memory 8Gb minimum (Recommended : 16Gb)
4. Storage: Minimum 256GB SSD/Flash Storage (Recommended: 512Gb)
5. Screen Size : 10.8” to 15.6” (Recommended: 11.6” – 13.3”)
6. Weight : Under 2kg (Recommended: under 1.6kg)
7. Battery Life : 6+ hours (During general use, not idle)
8. Input : Physical Keyboard/mouse, attached or detachable
9. Display Ports : HDMI
10. Other Ports : 1x USB, 3.5mm Headphone Jack

11. Wireless Network : Wi-Fi supporting wireless “N”, “AC” or “AX” standard  
(Recommended: Intel Network Adaptor with “AX” support)
12. Operating System: Microsoft Windows 11, Microsoft Windows 10 64Bit (English Language Only) or Apple macOS 11, 10.15 (English Language Only)
13. Language: English Language Only

### **Mandate for Music subjects**

1. Device Type: Laptop, notebook capable of supporting Microsoft Windows 11, Windows 10 or macOS.
2. Processor intel i5 or equivalent
3. Memory: 8Gb minimum (Recommended : 16Gb)
4. Storage: Minimum 256GB SSD/Flash Storage (Recommended: 512Gb)
5. Screen Size : 12” to 15.6”
6. Dedicated graphics card recommended
7. Weight : Under 2kg (Recommended: under 1.6kg)
8. Battery Life : 6+ hours (During general use, not idle)
9. Input : Physical Keyboard/mouse, attached or detachable
10. Display Ports : HDMI
11. Required Ports : at least 1x USB-A (normal USB), 3.5mm Headphone Jack
12. Wireless Network : Wi-Fi supporting wireless “N”, “AC” or “AX” standard  
(Recommended: Intel Network Adaptor with “AX” support)
13. Operating System:Microsoft Windows 11, Microsoft Windows 10 64Bit (English Language Only) or Apple macOS 11, 10.15 (English Language Only)
14. Accessories required:
  - a. Headphones
  - b. Sound Splitter - 3.5mm Stereo Audio To 2X 3.5mm Stereo Audio Splitter
  - c. USB-C to USB-A dongle for music keyboards (required for macbooks)

### **Minimum Required Software (Available for Download)**

- **Office Suite** : Microsoft Office 2016/O365 (provided by EDSC)
- **Anti-Virus** : Windows Defender (provided by EDSC)
- **Adobe** : Adobe CC 2021 (provided by EDSC)
- **Web Browser** : Google Chrome
- **PDF Reader** : Adobe Acrobat Reader DC

\*Additional requirements will be determined by chosen subjects/electives and communicated by teaching staff.

Refer to the 1-1 Digital Learning Program Timeline for information on device enrolment and software installation.

Further details and program updates will be posted on Compass School Manager: <https://edsc-vic.compass.education/>

### **Warranty/Insurance Recommendations**

- Additional 2-3 Years Warranty/Insurance recommended if available

# 1 to 1 Digital Learning Program Timeline

November 23

Bookings for Years 8 to 12 configuration open. Link will be published via the College News Feed.

Book via Trybooking:

<https://www.trybooking.com/BUCYK>

December 7

Bookings for Year 7 configuration open. Link will be published via the College News Feed.

Book via Trybooking:

<https://www.trybooking.com/BTHMU>

January 19, 20, 21

Year 7 Device Configuration.

Book via Trybooking:

<https://www.trybooking.com/BTHMU>

Directions will be provided on the day for device enrollment and software installation.

January 24

Years 8 to 12 Device Configuration.

Book via Trybooking:

<https://www.trybooking.com/BUCYK>

Directions will be provided on the day for device enrollment and software installation.

## Information Security

### Purpose

To make sure that schools manage and share information appropriately and securely in order to meet information security obligations and to appropriately protect staff, students and their families.

### Summary – critical information

- Information security aims to protect the confidentiality, integrity and availability of school information. This includes the consideration of privacy compliance when dealing with personal information. Refer to [Privacy Policy](#) for more information about privacy and information sharing.
- Principals must establish appropriate practices to protect critical and sensitive information. All staff should consider:
  - what information they have
  - how sensitive the information is
  - where it is stored
  - who has access to it.

Principals are to make sure that information security risks and issues are appropriately managed by seeking advice from the InfoSafe team.

### Policy

The following information provides an overview of the key practices schools must implement to protect the confidentiality, integrity and availability of school information.

For more detailed information on implementing these information security practices, refer to: [Information Security \(InfoSafe\): Guidance for Victorian Government Schools](#)

## **Behaviours – Being InfoSafe**

Schools must make sure that the protection of information is embedded in all aspects of school operations as outlined in this policy and accompanying Information Security Standards and guidance materials. The consequences of an information security breach can be far reaching, potentially affecting staff, students and families.

Priority Actions:

1. Ensure that priority actions from this policy are considered in appropriate local school practices and IT Committees.
2. Staff are encouraged to complete the [Information Security for School Staff eLearning module](#) (staff login required) on an annual basis.
3. Establish and maintain an InfoSafe culture by promoting this policy and through ongoing conversations.

## **Risks – Understanding your information risks**

Schools must adopt a risk-based approach to information security by periodically assessing themselves against a set of common, published risks and associated treatment plans. This will enable school treatment plans to be prioritised and actioned based on the extent of the risk.

Priority Actions:

1. Consider the IT environment, online tools and the nature of the information at your school.
2. Consider the most common school information security and privacy risks and their relevance at your school.
3. Refer to the [Pre-populated InfoSafe School Risk Document](#)

## **Access – Identify the appropriate access for the information at your school**

Schools must make sure that access to information is authorised for individuals based upon their role and function within the school environment. Failure to assign the right level of access to information to the right role may result in an information security or privacy breach.

Priority Actions:



1. Identify who has access to sensitive information and who has privileged accounts at your school. Refer to [Privacy Policy](#) for more information.
2. Establish a process to capture and regularly review school and Department staff, and third-party access, including parents, volunteers and contractors.
3. Establish a process to enforce need-to-know access to sensitive information (revoke access in a timely manner).

## **Incidents – Reporting incidents**

Schools must report any potential or confirmed information security incidents as soon as possible to the IT Service Desk 1800 641 943 or email [servicedesk@edumail.vic.gov.au](mailto:servicedesk@edumail.vic.gov.au) (or via their Specialist Technician) as soon as they are identified.

Problems that are not reported immediately can grow bigger and more difficult to contain, and early detection helps to mitigate any potential harms resulting from the incident. Some cyber-security incidents may also reveal a risk (such as a virus) that other schools can then prepare against.

Priority Actions:

1. Make sure all staff know what constitutes an information security incident.
2. Reinforce the importance to all staff of reporting incidents.
3. The principal must ensure that the incident is reported and then respond to the incident as advised by the Department.

## **Networks – Securing ICT networks**

Schools must maintain a secure ICT network by following Departmental requirements and adopting appropriate technical controls. Without these controls the school information and systems will be vulnerable to cyber-attacks.

Priority Actions:

1. IT Technicians in schools (whether engaged through the Technical Support to Schools Program or directly by the school) need to regularly review network configuration and anti-virus and patching arrangements as set out in the Tech Campus (login required, access limited to Department engaged technicians).

2. Technicians need to confirm the school's Internet Service Provider (ISP) arrangement meets the requirements of the DET standards.

## **Storage – Identifying and storing your information appropriately**

Schools must identify their critical and sensitive information and store it in approved and trusted locations.

Priority Actions:

1. Identify and document assets holding sensitive and critical information. Refer to [CASES21 Policy](#) for all mandated DET ICT school administration systems.
2. Refer to the [Pre-populated Risk Document](#) to assist with documenting assets. For systems holding personal information, ensure you have completed a Privacy Impact Assessment.
3. Refer to the [Privacy Policy](#) for information about Privacy Impact Assessments. Review school processes to identify where data is held long-term.

## **Physical – Physical protection**

Schools must protect information and ICT equipment by housing all ICT infrastructure (servers and network equipment) and personal computers, when not in use, in a locked and secured location with restricted access. Schools should also monitor visitor entry to the school premises and authorise entry into infrastructure and records storage locations.

Priority Actions:

1. Ensure the school follows both their local Visitors Policy and the Department's [Visitors in Schools Policy](#).
2. Make sure that sensitive information (digital and hard copy) and ICT equipment is housed in physically secured locations. Refer also to [Archives and Records Management Policy](#).

## **Awareness – Training and awareness**

Schools must encourage staff to be vigilant and aware of the ongoing need to protect sensitive school information and systems. Staff should complete the [Information Security for School Staff e-learning module](#) (staff login required). Schools should act on Department information and directions about emerging cyber security threats.

Priority Actions:

1. Continue to drive the completion rate of the Information Security for School Staff eLearning module and encourage all staff to complete the module annually.
2. Ensure the induction process for new staff, including contractors and casuals, includes the Information Security for School Staff eLearning module.
3. Regularly communicate, affirm and review security obligations for staff (and target specific roles that have access to sensitive information).

### **Sharing – Sharing information safely**

Schools must follow Department policies for sharing personal or sensitive information with other schools or anyone external to the school.

Priority Actions:

1. Identify which personal and sensitive information is regularly shared or likely to be shared (typically personal data of staff or students, but potentially other categories of information e.g. financial, commercial).
2. Refer to [Requests for Information about Students](#) and [Privacy Policy](#). Make sure staff are aware of Department policies and local procedures for sharing information.
3. Use only approved tools to transmit sensitive data, closely manage distribution lists.

### **Suppliers – Externally sourced systems security**

Schools and the Department must ensure the security of new systems and the suppliers who provide them.

Priority Actions:

1. Seek advice from the InfoSafe team to ensure all new systems meet Information Security and ICT security requirements.
2. For those systems holding personal information, conduct a Privacy Impact Assessment (PIA) which includes a security assessment for that system.

## Resources

For a range of resources and tools to support school with implementing this Information Security – InfoSafe Policy and associated standards and guidance material, refer to: [DET InfoSafe](#) on the Departmental intranet site (staff login required).

## Definitions

Information security incident

Indicators of a potential or actual information security incident are:

- emails from unexpected or unidentifiable senders
- unexpected emails from people that you do know
- requests for information from unknown sources
- Inability to access systems
- inability to access files or documents
- unusually slow systems or unexpected and strange behaviour of PCs and devices.

Personal information is recorded information or opinion about an identifiable individual. It can be almost any information linked to an individual, including name, address, sex, age, financial details, marital status, education or employment history. De-identified information about individuals can also be personal information if it has the potential to be re-identified.

Sensitive information for the purpose of this policy and associated guidance material, sensitive information in schools includes but is not limited to the following:

- student information including name address and date of birth
- student academic records, progress reports, assignments and assessments
- student health and medication information
- student information pertaining to family circumstances including Intervention Orders and Family Court decisions
- student class photographs and individual images
- parents' names, address, phone number, email address and custody instructions

- teachers' personal information
- parents' banking and credit card information and hard-copy records
- school financial information
- tendering and procurement documents
- vendor invoices, contacts and accounts payable and receivables.

## Related policies

- [Archives and Records Management](#)
- [Enrolment](#)
- [Privacy and Information Sharing](#)
- [Requests for Information about Students](#)

## Relevant legislation

- Privacy and Data Protection Act 2014 (Vic)
- Health Records Act 2001 (Vic)
- Victorian Data Sharing Act 2014 (Vic)
- Child Well Being and Safety Act 2005 (Vic)

## Contact

InfoSafe team at email: [infosafe@education.vic.gov.au](mailto:infosafe@education.vic.gov.au)