OAKLANDS CATHOLIC SCHOOL
AND
SIXTH FORM COLLEGE

With delegated responsibility from the Edith Stein Catholic Academy Trust

GENERAL INFORMATION COMMUNICATIONS TECHNOLOGY (ICT) POLICY

APPROVED BY BUSINESS AND COLLABORATION COMMITTEE	**22ND January 2018**
SCRUTINISED BY SENIOR LEADERSHIP TEAM	**15TH January 2018**
REVIEW DATE	**January 2018**
MEMBER OF STAFF RESPONSIBLE	**DIRECTOR OF BUSINESS AND FINANACE/HEAD OF IT AND TECHNICAL SUPPORT**
STATUTORY / NON-STATUTORY	**NON-STATUTORY**

Community Unity Opportunity

Document Management

Date	Details	Author	Approved By (Initials)
--	ICT Security Policy	Unknown	--
04/01/18	General ICT Policy combines the following previously published documents: • IT Security Policy • E-Safety Policy • Acceptable Use Policy (Staff) • Acceptable Use Policy (Student) • BYOD Policy (Student) • BYOD & School Device Policy (Staff) The later 4 documents have been renamed as protocols and will be appendices of the main policy document. The E-safety Policy will, for the time being, be an annex to the main policy. Otherwise the content has largely been copied and pasted. Headings, sub-headings and layout has been changed to ensure consistency. Contents table added to help with navigation Document Management table added to help keep track of changes	JD	

Contents

1.0 Introduction

1.1 As a Catholic school we recognise the power of ICT to enhance the operation and outcome of the school. As IT "advances further and further in the discovery of the resources and values contained in the whole of creation"[1], the Church often has declared her conviction that they are, in the words of the Second Vatican Council, "marvellous technical inventions"[2] that already do much to meet human needs and may yet do even more. Thus the Church has taken a fundamentally positive approach to technology. The Catholic Church also recognises that IT can be used inappropriately; therefore, the correct safeguarding and protections need to be enacted.

2.0 Scope of this Policy

2.1 This policy covers the general use and functionality of IT in the school. This should be read in conjunction with the Data Protection Policy. Data Protection covers both electronic and physical records and is therefore not appropriate for this document.

2.2 Although voice communications are due to move from a dedicated analogue telephone network to the schools' data network, voice is not covered in this policy.

3.0 Purpose of this Policy

3.1 The purpose of the Policy is to protect the schools' data, hardware and users from all threats, whether internal or external, deliberate or accidental. It is the policy of Oaklands Catholic School and Sixth Form College to ensure that as far as reasonably possible:

- regulatory and legislative requirements are met (also see the Data Protection Policy)
- the school is protected against loss of systems and/or data
- IT users are protected against inappropriate material, particularly when accessing the internet
- IT is used appropriately to deliver, within reason, the highest possible level of support to teaching and learning
- Users who choose to "bring your own device" (BYOD) to school are aware of the risks and agree to use equipment appropriately
- Users who benefit from a long term loan of school equipment, such as a laptop, are aware of their responsibilities

4.0 Policy Objectives

4.1 Against this background there are three main objectives of this policy:

- to ensure that equipment, data, network, staff, students and visitors are adequately protected against any action that could adversely affect them or the school;
- to ensure that users are aware of and fully comply with relevant legislation;
- to create and maintain within the school a level of awareness of the need for IT security to be an integral part of day to day operations and practices so that all staff understand the need for ICT security and their own responsibilities in this respect.

[1] 1] John Paul II, encyclical letter *Laborem Exercens*, n. 25; cf. Vatican Council II, Pastoral Constitution on the Church in the Modern World *Gaudium et Spes*, n. 34.

[2] [2] Vatican Council II, Decree on the Means of Social Communication *Inter Mirifica*, n. 1.

5.0 Definitions

5.1 For the purposes of this document the following terms are defined:

- **Client**: any electronic device that connects to the network.
- **Network**: the infrastructure over which clients communicate or access data.
- **Data**: any information stored or processed within the network, including text, pictures and sound
- **Software**: programmes or applications that are used to access, present, or create data.
- **User[s]**: applies to any School employee, student or other authorised person who uses the school's network.
- **The School**: Oaklands Catholic School and Sixth Form College.
- **Network Services**: Services available on the school's secure network, such as printing, access to shared directories, or access to other school data.

6.0 Policy Application

6.1 All staff and students working for or attending the school are required to return a signed Acceptable Use Protocol before they are granted access to the network. Other users, such as guests or visitors are permitted to use the school network to access filtered internet content, but may not use other network services.

6.2 A member of SLT may at their discretion allow a student to access the network for a temporary period at the start of term, pending the return of a signed Acceptable Use Protocol. The Acceptable Use Protocol for staff is available as Appendix 1. Appendix 2 shows a similar protocol for Students. Sixth Form students wishing to bring in a personal device are also required to complete a BYOD form, available as Appendix 5.

6.3 A member of staff, usually a Teacher, may require the use of a laptop supplied by the school. This is subject to a number of terms and conditions, which are detailed in Appendix 4.

6.4 Finally, the school places a high priority on keeping students safe. To this end, the school's e-safety guidance is given in Appendix 3.

7.0 Risks

7.1 At the time of writing, the school is aware that substantial changes are due to come into force with the General Data Protection Regulations (GDPR) which will be enforced by the Information Commissions Office (ICO) in May 2018. Although the principals and general direction of GDPR is known, the Government has still to make clear the final details of these regulations.

7.2 A further risk is the change from an analogue network to a digital network for voice communications. This may impact the schools; data network and future changes to this policy may be required.

7.3 Finally, although Sixth Form students are permitted to bring in their own devices, other students are currently prohibited from doing so. This may change and it is anticipated that the students' Parent/Carer will then be required to sign a BYOD agreement, similar to the one already used by Sixth Form students (Appendix 5).

8.0 Roles and Responsibilities

8.1 ICT security relies on management and user actions to ensure that its aims are achieved. Consequently, roles and responsibilities are defined below.

8.2 **Ownership**

8.2.1 The owner has the legal title to the property. In this respect, all software, data and associated documentation produced in connection with the work of the school are the legal property of Edith Stein Catholic Academy Trust (ESCAT). Exceptions to this will be allowed for software and documentation produced by individual teachers for lesson purposes – this includes schemes of work, lesson plans, worksheets or as otherwise agreed in writing by the Headteacher.

8.2.2 Software Licencing
Some software titles and data that are the legal property of external organisations are acquired and used under contract or licence. It is the school's policy that all software is properly licenced in accordance with the vendor's requirements.

8.2.3 Software Updates & Patches
Where security patches are released for specific software titles, such as Microsoft Office, they should be applied within a reasonable time frame. Older software that is no longer updated by the manufacturers may represent a security risk to the school. Use of such software should be phased out and replaced with up to date software as appropriate.

8.3 **Local Governing Body**

The local governing body, on behalf of the Trustees of ESCAT, has the responsibility for ensuring that the school complies with the legislative requirements relating to the use of IT systems and for disseminating policy on IT security and other IT related matters. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.

8.4 **Headteacher**

8.4.1 The Headteacher is responsible for ensuring that the legislative requirements relating to the use of IT are met and that the school's General ICT Policy, is adopted and maintained. He/she is also responsible for ensuring that any special security measures relating to the school's IT facilities are applied and documented as an integral part of the Policy.

8.4.2 In practice, the day to day functions should be delegated to the 'Network Manager', who must be nominated in writing by the Headteacher. This would take the form of an item in a job description.

8.4.3 The Headteacher is responsible for ensuring that the Data Protection requirements are complied with fully by the school. See the separate Data Protection Policy for further details.

8.4.4 In addition, the Headteacher is responsible for ensuring that users are familiar with the relevant aspects of both this Policy and the Data Protection Policy and to ensure that the appropriate controls are in place for staff. This is particularly important with the increased use of devices away from the Oaklands campus.

8.5 **Network Manager**

8.5.1 The Network Manager is responsible for the school's IT devices, network, data, and software and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection. The Network Manager will be an employee of the school.

8.5.2 The Network Manager will administer the practical aspects of IT protection and ensure that various functions are performed, such as ensuring data is backed and can be restored, Disaster Recovery is available, access to the network is secure.

8.5.3 In line with these responsibilities, the Network Manager will be the official point of contact for IT security issues and as such is responsible for notifying the Headteacher or Chair of Governors of any suspected or actual breach of IT security occurring within the school. The Headteacher or Chair of Governors should ensure that details of the suspected or actual breach are recorded and made available to Internal Audit upon request. The Headteacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity.

8.5.4 It is vital, therefore, that the Network Manager is fully conversant with the General ICT Policy and Data Protection Policy and maintains an up to date knowledge of best practice and follows the associated approved practices.

8.6 **School IT Support Technicians**

The school technicians are responsible for maintaining, repairing and proactively supporting IT resources as directed by the Network Manager. The school technicians will also monitor the network for breaches of security and inform the Headteacher or Network Manager.

8.7 **Users**

8.7.1 All users of the school's network must comply with the requirements of this Policy and the Data Protection Policy.

8.7.2 Users are responsible for notifying the Network Manager of any suspected or actual breach of security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Governors or to the Director of Business and Finance.

8.7.3 Users are responsible for the equipment they use including:

- Physical security
- Security of data
- Their own passwords

8.7.4 Users issued with a school device, such as a laptop, are further required read, sign and return a "Staff Device Protocol" (Appendix 5). By doing so, they are required to take custodianship of the device, look after it, use it properly and safely, and return it on request.

8.7.5 Where users are students, the school's information management system (SIMS) will define who is granted access to the network. Where a user is a member of staff, it is the HR Office Staff and the appropriate Head of Department who are jointly responsible for informing IT Support of starters, leavers or staff who are changing roles.

8.7.6 Users who regularly access the school's IT Networks, such as staff and students, are required to sign and return Acceptable Use Protocol agreements (Appendix 1 & 2). Other users, such as visitors may use the network to access the internet, but not other network resources.

9.0 Legislation

9.1 The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of IT systems, which comprise principally of:

- Data Protection Act (1998)
- Computer Misuse Act (1990)
- Copyright, Designs and Patents Act (1988)
- The Telecommunications Act (1984)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)
- General Data Protection Regulations (2018)

9.2 It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

9.3 Data Protection requirements are confirmed in the school's Data Protection Policy.

9.4 **Computer Misuse Act (1990)**

9.4.1 Under the Computer Misuse Act (1990) the following are criminal offences, if undertaken intentionally:

- Unauthorised access to a computer system or data;
- Unauthorised access preparatory to another criminal action;
- Unauthorised modification of a computer system or data.

9.4.2 All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of school policy and may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

9.5 **Copyright, Designs and Patents Act (1988)**

9.5.1 The Copyright, Designs and Patents Act (1988) provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.

9.5.2 Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.

9.5.3 All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.

9.5.4 The Network Manager is responsible for compiling and maintaining an inventory of all software held by the School and for checking it at least annually to ensure that software licences accord with installations. To ensure that we comply with the Copyright, Designs and Patents Act 1988 users must get prior permission in writing from the Network Manager before copying any software.

9.5.5 All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

9.6 **The Telecommunications Act (1984) and the Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations (2000)**

9.6.1 The Telecommunications Act 1984, section 43 makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character'.

9.6.2 The Telecommunications Regulations 2000 impose restrictions on the interception of communications such as e-mail.

10.0 Management of the Policy

10.1 Sufficient resources should be allocated each year to ensure the security of the school's IT systems and to enable users to comply fully with the legal requirements and policies covered in this policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Governors/Directors by the Headteacher.

10.2 Suitable training for all regular IT users and documentation to promote the proper use of ICT systems will be provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. A record of the training provided through the school to each individual user will be maintained.

10.3 In addition, users will be made aware of the value and importance of IT networks and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for IT security.

10.4 To help achieve these aims, the relevant parts of the General ICT Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be available to users.

10.5 The Headteacher must ensure that adequate procedures are established in respect of the IT security implications of personnel changes. Suitable measures should be applied that provide for continuity of IT security when staff vacate or occupy a post. These measures as a minimum must include:

- a record that new staff have been issued with, have read the appropriate documentation
- staff & students have signed the appropriate Acceptable Use Protocol
- users issued with a Laptop have signed the Staff Device Protocol
- a record of the access rights to systems granted to an individual user and their limitations on the use of the data in relation to the data protection registrations in place
- a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment.

11.0 Physical Security

11.1 Location Access

11.1.1 Adequate consideration should be given to the physical security of rooms containing IT equipment (including associated cabling). Only authorised persons are admitted to rooms that contain servers, which must be locked when unattended.

11.1.2 The Network Manager must ensure appropriate arrangements are applied for the removal of any IT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

11.2 Equipment siting

11.2.1 Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

- devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- equipment is sited to avoid environmental damage from causes such as dust & heat;
- users have been instructed not to leave computers logged-on or unlocked when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users;
- users have been instructed not to leave hard copies of sensitive data unattended on desks.

11.2.2 The same rules apply when accessing the network or data when away from the school campus.

11.3 Inventory

The Network Manager shall ensure that an inventory of all IT equipment is maintained and all items accounted for at least annually.

12.0 Legitimate Use

12.1 The school's ICT facilities must not be used in any way that breaks the law. Such breaches include, but are not limited to:

- making, distributing or using unlicensed software;
- making or sending threatening, offensive, or harassing messages;
- creating, possessing or distributing inappropriate material;
- unauthorised personal use of the school's computer facilities.

12.2 Private Hardware & Software

Dangers can occur from the use of unlicensed software or devices infected with malware. It is therefore vital that any private software permitted to be used on the school's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for school purposes must be approved by the Network Manager or a member of SLT.

12.3 **IT Security Facilities**

Consideration should be given to including appropriate processing controls such as audit trails, input validation checks, control totals for output, reports on attempted unauthorised access, etc. For new systems, such facilities to be confirmed at the time of installing the system.

12.4 **Authorisation**

12.4.1 Staff and Students are automatically authorised the use the school network and access appropriate resources, on receipt of a signed Acceptable Use Protocol. Guest users may be granted access to further network resources at the discretion of the Network Manager or a member of SLT.

12.4.2 Failure to establish the limits of network access may result in the school being unable to use the sanctions of the Computer Misuse Act (1990). Not only will it be difficult to demonstrate that a user has exceeded the authority given, it will also be difficult to show definitively who is authorised to use a computer system.

12.4.3 Where IT systems are available for use, messages should be displayed to users warning against unauthorised use of the system. This may take the form of warnings displayed by the IT system itself, the use of wall displays or other display suitable to that environment.

12.4.4 Access eligibility will be reviewed continually. In particular, network access will be removed when a member of staff leaves the employment of the school or when a student leaves the school. Network access will be reviewed whenever a member of staff changes roles.

12.4.5 Failure to change access eligibility and passwords will leave the network vulnerable to misuse.

13.0 Passwords

13.1 The level of password control will be defined by the Network Manager based on the value and sensitivity of the data involved, including the use of “time out” passwords where a terminal/PC is left unused for a defined period.

13.2 Passwords for staff users should be changed at least annually not be re-used within 5 years. They should be a minimum of 8 characters, including a mix of letters and numbers.

13.3 Staff passwords must not be written down.

13.4 Passwords must protect access to all IT systems. On school owned clients, the Basic Input/Output System (BIOS) should be protected with a password to restrict unauthorised access.

13.5 A password must be changed if it is suspected that a breach of security may have occurred.

13.6 There is a possibility that such a breach could occur when:

- a password holder leaves the school or is transferred to another post;
- a password may have become known to a person not entitled to know it.

13.7 The need to change one or more passwords will be determined by the risk of the security breach.

13.8 Users must not reveal their password to anyone. Users who forget their password must request the Network Manager issue a new password.

13.9 Passwords or other data replicated to 3rd parties (such as external websites) remain the responsibility and property of the school. The security of any such 3rd parties should be checked and considered prior to any agreement to use their services.

14.0 Security of the Network

14.1 Only devices approved by the IT Network Manager should be permitted to be connected to the network, either through wired or wireless connectivity.

14.2. Where devices are connected to the network using wireless, the wireless network should be encrypted, and a user's login credentials should be validated prior to allowing network access.

14.3 **Encryption**

14.3.1 As a minimum, all devices of the ICT System that are portable should be fully encrypted.

14.3.2 Devices subject to encryption may include:

- Laptops
- PDAs
- Smartphones/Blackberries
- USB flash drives/Memory cards. (Note: the use of external storage such as flash drives are discouraged).

14.3.3 Where technology prevents the use of encryption (e.g. SD Memory Cards used in Digital Cameras), then data subject to the Data Protection Act must not be stored on these devices.

14.3.4 When using encryption systems that require a password to access the system, the same guidance for passwords outlined earlier applies.

14.4 **Filtering of the Internet**

Access to internet resources is filtered using an approved system. It is the responsibility of the Network Manager to monitor the effectiveness of filtering at the school and report issues to the Director of Business and Finance. Where breaches of internet filtering have occurred, the Network Manager should inform the Headteacher and assess the risk of continued access.

15.0 Backup and Disaster Recovery

15.1 Backups are copies of data, which can be restored should the original data be lost (for example, if a file has been deleted in error). Disaster Recovery will recover IT Servers that are down due to a major incident, such as a fire in a server room.

15.2 **Backups**

15.2.1 Backups contain data that must be protected and should be clearly marked as to what they are and when they were taken. They should be stored away from the system to which they relate and kept for an appropriate period of time. This is likely to be no more than 8 weeks.

15.2.2 Instructions for re-installing data or files from backup should be documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

15.3 **Disaster Recovery**

15.3.1 In order to ensure that essential services and facilities are restored as quickly as possible following a network failure, provision for Disaster Recovery must be in place on the school campus.

15.3.2 Where programs and data are held on external systems (such as 3rd party websites) responsibility for backup remains with the 3rd party.

16.0 Operating System Patching

16.1 The Network Manager will ensure that all school owned clients and servers (physical or virtual) are patched on a regular basis to those releases distributed by the manufacturers of the operating systems. A record should be maintained of all machines running operating systems that can be patched along with each machine's patch status.

17.0 Virus Protection

17.1 The school will use appropriate anti-virus software for all school owned devices.

17.2 All Users should take precautions to avoid malicious software (malware) that may destroy or corrupt data.

17.3 The school will ensure that every user is aware that any device with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the Network Manager who must take appropriate action, including removing the source of infection.

17.4 The ESCAT could be open to a legal action for negligence should a person suffer as a consequence of a computer virus on school equipment.

17.5 Any third-party laptops are not normally granted access to the main school network. They may be granted guest access to a separate network which is logically separate from the "STUDENT" domain to allow connection to the internet.

17.6 The school will ensure that up-to-date anti-virus signatures are applied to all servers and that they are available for users to apply, or are automatically applied, to PCs or laptops.

18.0 Disposal of Waste

18.1 Disposal of waste ICT media such as print-outs, USB sticks will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.

19.0 Disposal of Equipment

19.1 The Data Protection Act requires that any personal data held on a part of the ICT system subject to disposal is to be destroyed.

19.2 Prior to the transfer or disposal of any ICT equipment the Network Manager must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data by having ADISA Certification. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in the school's Finance Policy and statutory Financial Regulations apply. Any IT equipment must be disposed of in accordance with WEEE regulations.

19.3 It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently. The school should maintain a regularly updated asset register of licenses and should indicate when licenses have been transferred from one part of the ICT system to another.

20.0 Repair of Equipment

20.1 If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on other secure media for subsequent reinstallation, if possible. The school will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

21.0 Data/SIMS

21.1 There are 2 types of data held in SIMS (Schools Information Management System):

21.1.1 Personal Data

- Names
- Date of Birth
- Gender
- Address
- Telephone numbers and email addresses
- Mother's maiden name
- Unique Pupil Number (UPN)
- Teacher number
- Photograph

21.1.2 Sensitive Data

- Contact and next of kin details
- Ethnicity
- Disability and medical issues
- Pupil free school meal eligibility
- Pupil Special Educational Needs details
- Pupil in Care/Child Protection Register details
- Pupil assessment data and reports

21.2 The necessary authority given to staff to access SIMS is given by the SIMS Manager and is sufficient but not excessive.

21.3 A minimum of 2, but no more than 3 school staff have access to the SIMS System Manager program. The following roles have been nominated by the Headteacher:

- Deputy Headteacher
- SIMS Manager
- SIMS Assistant

21.4 SIMS System Manager roles have the following authority and functions:

- To manage SIMS user accounts and permissions
- To ensure that SIMS users have individual user logins in their own names
- To create SIMS login accounts for new SIMS users
- To add or remove permissions for a user to different areas of SIMS
- To reset a user's SIMS login if a password is forgotten
- To disable the SIMS login when a member of staff leaves

22.0 Security Incidents

22.1 All suspected or actual breaches of IT security shall be reported to the Network Manager or the Headteacher in their absence, who should ensure a speedy and effective response to be made to an IT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the IT service quickly. All reported breaches of IT security are to be reported to the Local Governing Body though the Business and Collaboration Committee.

22.2 The Audit Commission's Survey of Computer Fraud and Abuse (1990) revealed that over 50% of incidents of ICT misuse are uncovered accidentally. It is, therefore, important that users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

22.3 It should be recognised that the school and its officers may be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of IT security within the school where insufficient action had been taken to resolve the breach.

23.0 Network/Internet Acceptable Use Protocol

23.1 The school's Acceptable Use Protocol applies to all school staff, students and third parties who use school facilities. The protocol covers the use of e-mail, the Internet, services accessed through the Internet and local file and network usage. The conditions of use are explained in the protocol. All school staff accessing these facilities must be issued with a copy of the Acceptable Use Protocol and other relevant documents and complete the user agreement attached to the protocol. For all students, the school will ensure that the relevant 'Acceptable Use Protocol' document is issued and the consent form is completed by pupils and their parents. Copies of the Protocol can be found in Appendix 1 &2.

24.0 Personal Use

24.1 The School has devoted time and effort into developing IT systems to assist employees with their work. It is, however, recognised that there are times when staff may want to use the network for non-work related purposes, and in recognising this need the School permits staff to use the network for personal use, subject to some restrictions.

24.2 Systems must not be used for personal use during working hours. Employees must not allow personal use of systems to interfere with their day to day duties. Any non-job related use of the systems during working hours may be subject to disciplinary action.

24.3 Employees must not use software licenced by the school for personal use unless permitted under the terms of the licence. Employees are responsible for checking the licensing position. Microsoft Office and Internet Explorer are licensed for personal use.

25.0 Disciplinary Implications

25.1 Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in prosecutions of individuals & the School under the Computer Misuse Act (1990)

26.0 Data Security Monitoring

26.1 An annual audit of data security will include the following checks:

- Review of the permissions of users to all systems
- Check that new staff and students receive the school's ICT agreements
- Check that the school's ICO registration is current
- Review changes made to the data extracted from SIMS
- Review the school's URL filtering systems

27.0 Annex

E-Safety Policy

28.0 Appendices

1. Acceptable Use Protocol - Staff
2. Acceptable Use Protocol - Students
3. Staff Device Protocol
4. Bring Your Own Device (BYOD) Protocol - Students

Annex A – Oaklands E-Safety Policy

A1.0 Policy Statement

A1.1 Safeguarding is a serious matter; at Oaklands Catholic School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

A1.2 The purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met with an ongoing, secure and confident commitment
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to a member of staff, a visitor or a student or liability to the school.

A1.3 This policy is available for anybody to read on Oaklands Catholic School website; upon review within the staff handbook all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Protocol. A copy of this policy and the Students Acceptable Use Protocol will be sent home with students starting at the school year with a permission slip. Upon return of the signed permission with a slip and on acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

A1.4 The school will make every reasonable endeavour to provide a safe and secure environment of IT users. However, it should be noted that in an area where change is as fast paced as IT, where potential threats are identified constantly, users should not only obey the letter of this policy, but must comply with the spirit in which the policy is written.

A2.0 Policy Governance (Roles & Responsibilities)

A2.1 **Governing Body**

A2.1.1 The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least every 3 years and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- One governor will have overall responsibility for the governance of e-safety at the school and will:
    - Keep up to date with emerging risks and threats through technology use in order that appropriate challenge is undertaken where relevant
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents
    - Chair the e-Safety Committee

A2.2 **Headteacher**

A2.2.1 Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff (the e-Safety Officer). The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

A2.3 **e-Safety Officer**

A2.3.1 The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

A2.4 **ICT Technical Support Staff**

Technical support staff are responsible for ensuring that the IT infrastructure is secure; this will include at a minimum obeying the General ICT Policy, and that filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.

A2.5 **All Staff**

A2.5.1 Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.

A2.6 **All Students**

A2.6.1 The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

A2.6.2 E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

A2.7 **Parents and Carers**

A2.7.1 Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, website and school newsletters the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

A2.7.2 Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

A2.8 **e-Safety Committee**

A2.8.1 Chaired by the Governor responsible for e-Safety, the e-safety Committee is responsible:

- to advise on changes to the e-safety policy.
- to establish the effectiveness (or ~~not~~ otherwise) of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

A2.8.2 Established from volunteer students, parents, e-Safety Officer, responsible Governor and others as required, the e-Safety Committee will meet on a termly basis.

A3.0 Technology

A3.1 Oaklands Catholic School uses a range of devices including PCs, laptops and Apple Macs. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

A3.1.1 <u>Internet Filtering</u>

We use Fortigate UTM firewall and filtering software that is intended to prevent access to inappropriate websites. Whether a website is deemed appropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Network Manager, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

It should be noted that no content filter is 100% successful, and as such, users should immediately report any website or other content which makes them uncomfortable to the appropriate person. Immediate action can be taken to prevent any further access.

A3.1.2 <u>Email Filtering</u>

The school uses Microsoft Office 365 and BitDefender software that prevents any infected email to be sent from or received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

A3.1.3 Encryption

All network clients that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB drives) is to be brought to the attention of the Headteacher immediately. The Headteacher will take advice and decide whether a report needs to be made to the Information Commissioner's Office.

A3.1.4 Passwords

All staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a regular basis or if there has been a compromise, whichever is sooner. The network manager and IT Support will be responsible for ensuring that passwords are changed.

A3.1.6 Anti-Virus

All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals are to be scanned for viruses before use.

A3.1.7 Monitoring

Student use of computers is monitored. Any inappropriate words typed by students are logged and reported to the IT Support team, who will escalate to Form Teachers, Heads of Year, or Safeguarding Officers as appropriate.

A4.0 Safe Use

A4.1 **Internet**

Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing the staff Acceptable Use Protocol; students upon signing and returning their acceptance of the Acceptable Use Protocol.

A4.2 **Email**

A4.2.1 All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

A4.2.2 Students are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of their forename and surname, e.g. forename.surname@oaklandscatholicschool.org

A4.3 **Photos and videos**

Digital media such as photos and videos are covered in the Schools' Imagery Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

A4.4 **Social Networking**

A4.4.1 There are many social networking services available; Oaklands Catholic School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Oaklands Catholic School and have been appropriately risk assessed. Should staff wish to use other social-media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below).
- Facebook – used by the school as a broadcast service (see below)
- Office 365 SharePoint Service (such as Yammer).

A4.4.2 A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

A4.4.3 In addition, the following is to be strictly adhered to:

- Permission slips (via the School's Imagery Policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

A4.5 **Notice and take down policy**

Should it come to the schools' attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

A4.6 **Incidents**

Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

A4.6 **Training and Curriculum**

A4.6.1 It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Oaklands Catholic School will have an annual programme of training which is suitable to the audience.

4.6.2 e-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning through ICT lessons in Years 7-9 for all Oaklands students.

A4.6.3 As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

A4.6.4 The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

A4.6.5 The e-Safety Training Programme can be found in the e-safety folder within the Staff Only drive on the school network

A5.0 Why we Filter the Internet

A5.1 Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the e-safety toolbox that is of particular importance. When talking about an Internet filter there are two important aspects, very broadly speaking:

- **Filtering** - this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.
- **Monitoring** - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

A5.2 **Why do we Filter and Monitor?**

Schools filter Internet activity for two reasons:

A5.2.1 We filter to ensure

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

A5.2.2 We monitor for assurance

- All staff, students and parents of students will be informed that Internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites.
- (as much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

A6.0 A right to privacy?

Everybody has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this guide, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business.

Appendix 1
Acceptable Use Protocol - Staff

B1.0 Introduction

B1.1 As a caring, professional organisation with responsibility for children's safeguarding it is important that all staff at Oaklands take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All staff should act in a Christian manner whilst using the school computers, as reflected in the schools' ethos.

B1.2 This protocol should be read in conjunction with the General ICT Policy and the Staff Device and BYOD Protocols.

B2.0 Aims

The aims of this protocol are:

- To enable management and governors to accept responsibility in ensuring that computer systems and the internet within school are used in a respectful manner by all staff.
- Provide a framework that allows any cause for concern to be taken seriously.
- To clarify to staff expectations when using the school computer systems and the internet.
- To encourage an environment that recognises the advantages of using computers and the internet.
- To give staff the right to be safe and protected while using the schools' computer system.
- To give staff positive advice and guidance.

B3.0 School Policy

B3.1 This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

B3.2 The school's Information Systems include networks, data and data storage, online and offline communication technologies and access devices such as desktops, laptops, mobile phones, digital cameras, email and social media sites**.**

B3.3 School owned information systems must be used appropriately. The Computer Misuse Act 1990 makes the following criminal offences:

- to gain unauthorised access to computer material
- to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation

B3.4 Staff should avoid storing personal information on the school computer system that is unrelated to school activities, such as personal photographs or financial information.

B3.5 Staff must respect copyright and intellectual property rights.

B3.6 Staff must read and understand the school e-Safety policy at Annex A to the General ICT Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

B3.7 Staff must not attempt to bypass any filtering and/or security systems put in place by the school.

B3.8 If there is a suspicion that a computer or system has been damaged or affected by a virus or other malware or if any school related documents or files have been lost, staff must report this to the ICT Support Team as soon as possible using the usual contact methods.

B3.9 Electronic communications with pupils, parents/carers and other professionals should only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership Team.

B3.10 The use of ICT and information systems must always be compatible with the users' professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. Personal use of ICT must not interfere with work duties.

B3.11 Staff must not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or do anything which could bring their professional role or the school into disrepute.

B3.12 Each member of staff should promote e-Safety with the students and colleagues and help others to develop a responsible attitude to safety online, system use and to the content they access or create.

B3.13 Staff must ensure that students, other than 6th Form Students, accessing the internet are properly supervised.

B3.14 Any queries or questions regarding safe and professional practise online either in school or off site, should be raised with the e-Safety Coordinator or the Headteacher.

B4.0 Sanctions

B4.1 The misuse of school's computer systems by a member of staff will be reported to the Headteacher. By failing to follow the acceptable use protocol you could be subject to disciplinary action. This could include a warning, suspension, referral to governors and in the event of illegal activities the involvement of the police.

B4.2 *The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Protocol and the School's Data Protection Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects unlawful storage of text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.*

B5.0 Agreement

I have read, understood and agree to comply with the Staff ICT Acceptable Use Protocol

Signed ……

Print Name ……

Date ……

Accepted by: ……..……..……

Appendix 2
Acceptable Use Protocol – Students

C1.0 Introduction

C1.1 All students must follow the conditions described in this protocol when using school ICT network or resources, such as email or school websites.

C1.2 Breaking these conditions may lead to:

- Withdrawal of the students' access
- Close monitoring of the students' network activity
- Investigation of the students past network activity
- In extreme cases, criminal prosecution

C1.3 Students will be provided with guidance by staff in the use of the resources available through the school network. School staff will regularly monitor the network to make sure that it is being used responsibly. The school will not be responsible for any loss of data as a result of system failure or student mistakes in using the system. Use of any information obtained via the network is at the student's own risk.

C2.0 Conditions of Use

Student access to network resources is a privilege, not a right. Students will be expected to use the resources for the educational purposes for which they are provided. It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this Protocol. Students must also accept personal responsibility for reporting any misuse of the network to a teacher or the IT Support Team.

C3.0 Acceptable Use

C3.1 Students are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All use must be consistent with the school ethos and code of conduct.

C3.2 When using email, Students must:

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer and furthermore infect the network causing major problems for all users.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

C3.3 By signing this protocol, you agree to the following:

1	**When using school equipment, I will treat it with respect and report any faults or breakages to an appropriate member of staff**
2	I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school into disrepute.
3	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
4	I will not use language that could incite hatred against any minority group.
5	I realise that files held on the school network will be regularly checked by the IT Support Team or other members of staff.
6	I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
7	I will not trespass into other users' files or folders.
8	I will not share my login details (including passwords) with anyone else. I will never use somebody else's username and password.
9	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact a teacher or the IT Support Team.
10	I will ensure that I log off properly after my network session has finished.
11	If I find an unattended machine logged on under other users username I will not continue using the machine and I will log it off immediately.
12	I understand that I am not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
13	I am aware that e-mail is not guaranteed to be private. Messages supporting illegal activities will be reported. Anonymous/unnamed messages are not permitted.
14	I will not use the network in any way that would disrupt use of the network by others.
15	I will report to a teacher any accidental access to other people's information, unsuitable websites or if I am sent inappropriate materials that make me feel uncomfortable.
16	I will not introduce "USB drives" or other portable devices into the network without checking them for viruses first.
17	I will not attempt to visit websites that might be considered inappropriate or illegal.
18	I will not receive, send or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting.
19	I understand that unapproved system utilities and executable files are not allowed in my work areas or attached to e-mails.
20	I agree to comply with the acceptable use protocol of any other networks that I access.

C4.0 Unacceptable Use

C4.1 Examples of unacceptable use include, but are not limited to:

- Creating, transmitting, displaying or publishing any material, such as text, images or sounds that are likely to harass, cause offence, inconvenience or cause needless anxiety to any other person.
- Unauthorised access to data and resources on the school network system that belong to other users.

C4.2 User action that would cause:

- Corruption or destruction of other users' data,
- Violate the privacy or dignity of other users,
- Intentionally waste time or resources on the school network or elsewhere.

C5.0 Email

Students must not:

- Email information that could cause damage or a danger of disruption
- Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person
- Knowingly or recklessly email false or defamatory information about a person or organisation
- Forward an email that was sent privately without permission of the person who sent the message
- Email private information about another person
- Email chain letters or engage in "spamming"
- Use email in lessons without permission from the member of staff taking the lesson

C6.0 Network Security

You must never log in with another person's user ID and password, or use a machine left unattended, but logged in by another user. If you discover a security problem, for example being able to access another user's data, you must inform a teacher or a member of the IT Support Team immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

C7.0 Instructions

Please keep a copy of the Acceptable Use Protocol for your records. Please sign and return the agreement in the section below.

C8.0 Agreement

<table>
<tr><td colspan="2">All pupils use computer facilities including internet access and email as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/guardian are asked to sign to show that the school's Acceptable Use Protocol has been understood and agreed.</td></tr>
<tr><td>Student: [Print Name]</td><td>Tutor Group:</td></tr>
<tr><td colspan="2">Student's agreement
I have read, understand and agree to abide by the school's acceptable use protocol.
I will use the computer and network technologies in a responsible way at all times.
I know that network, internet and email use may be monitored.</td></tr>
<tr><td>Signature:</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/Guardian's consent

I have read and understood the school acceptable use protocol agreement and give permission for my son/daughter to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.
I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.</td></tr>
<tr><td>Name: [Print Name]</td><td>Date:</td></tr>
<tr><td colspan="2">Signature:</td></tr>
</table>

Appendix 3
Staff Device Protocol

D1.0 Introduction

Within our Christian family we strive to achieve the highest standards by creating a school that enables us to serve the school community by participation, support and contribution to the common good and by good husbandry of valuable resources. It is important individuals are kept safe and are cared for.

D2.0 Purpose of this document

D2.1 All members of staff who have been allocated a school computing device, such as a laptop, need to be aware of Oaklands Catholic School and Sixth Form College's protocol for the use of that device.

D2.2 In addition, we are currently finding more members of staff are choosing bring personal IT devices to school and are requesting access to school resources, such as the wireless network, and an internet connection. While this is acceptable, the relevant sections of this protocol must be followed. The school reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

D2.3 The objectives of this document are to:

- ensure that the person allocated a school device assumes an appropriate level of responsibility for school property
- ensure the safe use of personal devices
- ensure that all mobile devices are maintained in a secure environment and that the risk of loss or theft is minimised
- provide guidance on the care of mobile devices
- provide health & safety advice on the use of mobile devices

D3.0 Scope

D3.1 This protocol applies to all mobile computing devices that are either purchased by school or that members of staff have chosen to bring to school. These devices may include laptop computers, tablets, netbooks, smartphones or other equipment.

D4.0 School Owned Devices

D4.1 This section applies to devices purchased by the school and allocated to members of staff.

D4.2 Ownership
While a device may be allocated to an individual member of staff, the equipment remains the property of the school at all times. The individual to whom a device has been allocated must sign and comply with this agreement. When the device is allocated, the individual assumes temporary custodianship.

D4.3 Surrender of the Device

The devices must be returned immediately to the IT Support Team either

- at the end of a lease agreement or
- at the end of a contract of employment with the school or
- at the start of an extended absence from the school, such as illness or maternity leave (arrangements may necessary for long term cover to have access to the device) or
- at any other time requested by the ICT Support Team It may be necessary to recall the devices from time to time to allow for maintenance and upgrades. Custodians will be given reasonable notice and any downtime will be kept to a minimum.

D4.4 Responsibility

The device, together with any data stored on it, is the sole responsibility of the named custodian to whom it has been allocated until returned to the IT Support Team. If a custodian lends it to a third party or allows its misuse, it is still considered to be the custodians' responsibility.

D4.5 Identification

The device will have a reference number attached to the case. This should not be removed.

D6.0 Custodian's responsibilities

D6.1 This section contains information about procedures that must be followed, together with guidance on procedures that custodians are advised to follow.

D6.2 Carrying devices

Devices should always be carried in the protective bag supplied. In wet or rainy conditions, devices **MUST** be transported in their protective bags.

D6.3 Screen care

Device screens can be damaged if subject to rough treatment. The screen is particularly sensitive to damage from excessive pressure. In general, it is best to avoid touching the screen all together. To avoid damage to the screen:

- do not lean on the top of the device when it is closed
- do not place anything in the carrying case that will press against the cover
- do not place anything on the keyboard – forgetting objects on the keyboard and closing the lid may cause damage to the screen
- clean the screen with soft, dry cloth or anti-static cloth

D6.4 Warranty

All devices are supplied with a minimum of a one-year manufacturer's warranty covering parts and labour. Custodians **MUST** take care not to invalidate the warranty due to:

- accidental damage
- unreasonable use, abuse, neglect and alterations
- improper service, installation, or connection to peripherals
- attempting to dismantle or repair the device or install modifications

D6.5 Maintenance of the equipment is the responsibility of the ICT Support Team. All maintenance issues **MUST** be referred immediately to the ICT Support Team.

D6.6 Software

D6.6.1 Custodians must take reasonable steps to protect against the installation of unlicensed or malicious software. The IT Support Team can supply information about licensing agreements for school software.

D6.6.2 All installed software **MUST** be covered by a valid license agreement held by the school.

D6.6.3 Software installation should be carried out by the IT Support Team.

D6.6.4 When equipment is to be used to access the internet other than by the school broadband connection users **MUST** ensure that spyware protection software, antivirus software and a firewall are installed and working. Connection to the internet should not be by wireless router, unless the wireless connection signal (SSID) is password protected.

D6.6.5 No software should be removed, uninstalled or disabled under any circumstances.

D6.6.6 Any software problems should be reported through the usual support channels.

D6.6.7 Protective software **MUST** be updated regularly. For laptop computers, it will be necessary to connect them to the school network to update the antivirus software. This should be done regularly with updates continuously added automatically during normal in school use.

D6.6.8 In general, Custodians are advised that the installation of a large number of software titles, including freeware and web browser toolbars, can lead to a degradation in the performance of a device and should be avoided unless absolutely necessary.

D7.0 Physical security

D7.1 Custodians are expected to protect school equipment from damage or theft and **MUST** take the following physical security preventative measures. Devices must not be:

- Left on view in an unattended vehicle, even for a short period of time
- Left in a vehicle overnight
- Left unattended and positioned so that the device is visible from outside a ground floor window

D7.2 When leaving a laptop unattended for any extended period, e.g. lunch breaks or overnight, users must physically secure it with a cable lock and/or lock it away in a robust cabinet or lock the door of an individually occupied office. Outside of school the custodian is responsible for ensuring the device is covered under household insurance policies.

D7.3 Data stored in the H: Drive or in “Work Folders” is automatically backed up on school servers. If a user also opts to backup data to a personal device, such as memory stick or external hard drive, they **MUST** ensure the backups are encrypted and kept secure. Encryption can be done using “BitLocker”. Further guidance can be obtained from the IT Support Team.

D7.4 To ensure laptops continue to work smoothly, it is strongly recommended that users keep no more than 50GB of data in their H: Drive or Work Folders.

D8.0 Personal use

D8.1 Limited personal use of school devices is permitted, subject to the restrictions contained in this or any other related policy. Any personal use is expected to be in the custodians own time and is not to interfere with job responsibilities.

D8.2 Where personal equipment, such as home printers, scanners etc. have been installed on a device, IT Support will not be responsible for any hardware or software support relating to the personal equipment and reserve the right to uninstall any software they consider to be affecting the performance of the device.

D9.0 Liability

Custodians will not be held responsible for any problems with a device resulting from regular school-related use or normal wear & tear; however, they may be held financially responsible for any problems caused by their negligence as deemed by the Headteacher.

Custodians may be held financially responsible for any school device stolen while in their care. The school reserves the right to audit the correct usage of the device at any time, and the custodian may be held liable for illegally held software or material in breach of copyright legislation.

Custodians are reminded that they should not deliberately seek out inappropriate or offensive materials on the internet and that they are subject to disciplinary procedures and the law of the land should they do so. Custodians are also advised to avoid websites likely to cause a virus or other security risk.

D10.0 Bring Your Own Device (BYOD)

D10.1 This section applies to members of staff who chose to bring a personal device in to school.

D10.2 Reason for this protocol
This protocol is intended to protect the security and integrity of the school's data and technology infrastructure. Limited exceptions to the protocol may occur due to variations in devices and platforms at the written discretion of the Headteacher.

D10.3 Support
The IT Support Team has limited support capabilities for BYOD, and unlike school-owned devices, they cannot undertake to fully support personal devices. The IT Support Team will make reasonable endeavours to support personal devices in the school, but priority will be given to school owned devices. This support is limited to troubleshooting a device for wireless connectivity to internet.

D10.4 Please note that if support is provided, the IT Support Team will have access to any personal information stored on the device. As part of supporting the device, it may be necessary remove data stored on the device or completely wipe the device if required. The school accepts no responsibility or liability for any loss incurred as a result.

D10.5 The school also reserves the right to remove any applications from a personal device that are considered to be a security risk to the school.

D10.6 Damages
The school is not responsible for any damages, insurance, theft or loss of a personal device on the school site. Any loss or damage to personal devices is the individual member of staff's responsibility, together with the provision of suitable insurance or protection.

D10.7 Data responsibility & backups
The school is not responsible for the backup or recovery of data on any personal device used at the school. The responsibility for data remains with the member of staff. The IT Support Team will not install any application software (e.g. iTunes) on school equipment for backing up data stored on a personal device. Sensitive data **MUST NOT** be stored on personal devices. This includes data relating to any living individual, organisational planning, budget papers etc. Staff should consult with the Head of IT if they are not sure what constitutes sensitive data.

D10.8 Security
Staff using a personal device and accessing school data or email **MUST** ensure the physical security of the device and immediately report any loss, theft or damage to the IT Support Team, and confirm whether any school data or email is stored on the device. Owners must ensure that all school data is permanently removed from devices prior to leaving employment at the school.

D10.9 Some mobile devices contain portable storage devices (PSD) such as flash memory cards that can be used to store data. Staff **MUST** ensure the physical security of privately owned PSD's if they contain school data. Staff should use data encryption on PSD's. The IT Support Team can provide advice about encryption options.

D10.10 Device owners **MUST** ensure that devices are updated regularly, including updates to applications and operating systems to the latest approved updates and security patches. Jail broken iOS or root broken Android Devices will not be permitted to connect to any school service.

D10.11 Personal devices are subject to the same Acceptable Use Protocol as school-owned devices.
Safety

D10.12 Staff should arrange for power adapters used in school to charge personal devices to be PAT tested before first use.

D11.0 General information

D11.1 This section applies to all mobile computer devices, irrespective of whether the device was purchased by the school, or brought in to school by a member of staff.

D11.2 Devices left unsupervised
Under no circumstances should a device be left unsupervised when it is logged on to the school network or logged in to SIMS. Users **MUST** either log off or lock the device if they are away from the device even for a short period.

D11.3 Devices displaying sensitive information (such as SIMS data) should be positioned so that the screen cannot be viewed by others.

D11.4 Users are advised to enable a screen saver password to guard against casual unauthorised usage. Staff using a personal device to access school data or email **MUST** have device password/PIN and timeout settings established on the device. The time out setting for the device to go into lock mode should not exceed 10 minutes.

D12.0 Password protection

D12.1 All devices storing school data **MUST** be password protected to guard against unauthorised usage. Where no data is stored on a device, users are advised to password protect the device. If a device has an "administrator" account, this **MUST** be password protected. For school owned devices, this will be set up by the IT Support Team.

D12.2 Users **MUST** change their password at least once a year and:

- never tell a password to anyone (except a member of the IT Support Team, on request)
- never write down a password
- never communicate a password by telephone, e-mail or instant messaging
- change a password whenever there is suspicion that it may have been compromised

D13.0 Data protection

D13.1 User **MUST** ensure they comply with data protection requirements on all devices. Note that data that is only for personal use is exempt; however, users **MUST** ensure that all reasonable measures have been taken to keep other users from accessing your file storage area.

D13.2 **Users should never allow Students to use any device that stores or has access to school data or email.**

D14.0 Do's and don'ts

D14.1 Please follow this general guidance to take care of computing devices:

- do take care not to bump or drop the device
- do take care when connecting/disconnecting power adapters, as the connection can be damaged easily
- do regularly delete files that no longer needed
- do empty your "Recycle Bin" regularly
- do not subject the device to extreme heat or cold
- do not expose the device to strong magnetic fields e.g. by placing next to loudspeakers
- do not keep files on your Desktop.
- do not place drinks or food in close proximity to the device
- never check in a device as luggage at an airport, and remember that x-rays can damage the devices' hard disk

D15.0 Health & safety

D15.1 The following advice provides some general guidelines for members of staff in the use of their mobile device.

D15.2 General advice
There are special health & safety issues associated with the use of mobile devices.

D15.2.1 Posture
Seating should be in a position which will prevent aches and pains in the small of the back or legs. An adjustable chair should be used which allows the user to sit so the lower part of the back is supported. Where this is not possible a cushion or pillow can be used to support the back of the user. When seated the user's forearms should be roughly horizontal when the hands are on the keyboard

D15.2.2 Use of a keyboard
Users should avoid any awkward bending of the wrists when using a keyboard. Sitting at the wrong height could lead to the wrists being in a bent position. Chairs should be positioned so that the forearms, wrists and hand are in a straight line. Arms resting on the work surface should keep the wrists in a relaxed, neutral position.

D15.2.3 Use of a mouse
Although many devices are supplied with an integral mouse, for prolonged usage it is best practice to use a separate mouse. If the laptop mouse is to be used then hands should be kept flat and the fingers relaxed when using a trackball, glide pad or nipple operated mouse.

D15.2.4 The screen

Glare and reflections on a computer screen should be avoided wherever possible. The angle of the screen can affect the amount of glare and reflection. A compromise may have to be made between glare, reflections and the most comfortable viewing angle. The device screen should be kept clean at all times.

D15.2.5 The environment

A mobile device, by definition, can be used in many differing operating environments.

If using it at home, then it is important to find a suitable place to work that has both a comfortable chair and a desk/table to place the device on.

If you use your laptop in a car you should sit upright in the passenger seat with the seat pushed well back. You can then rest the laptop on a flat surface such as a briefcase, which helps to raise the laptop height as well as giving an improved keying position for the wrists and hands.

The use of a laptop on trains and planes increases risk to the user due to lack of space. In most cases the device will have to be positioned close to the user and the poor posture that results may lead to the onset of aches and pains in the back, neck and forearm. This should be avoided.

If you are concerned about your working environment, a Display Screen Equipment (DSE) assessment should be conducted.

D16.0 Laptop and Staff BYOD Protocol Agreement

Please sign both the Staff and Admin copies of the Custodian Agreement.

I acknowledge that I have read and understood the terms and conditions detailed in this document. I accept that a charge may be levied against me if I do not comply with this protocol and, as a consequence, a school owned device needs repairs, is stolen, or that copyright has been breached. I acknowledge that if I choose to bring my own device to school it is at my own risk and I undertake to follow the protocol detailed in this document.

Model: _____

Reference #: _____

Date Loaned _____

Signature: _____

Print Name: _____

Please retain for your records

Appendix 4
Bring Your Own Device (BYOD) Protocol - Students

E1.0 Introduction

This protocol applies to students of Oaklands Catholic School Sixth Form College who have chosen to bring a personal device in to school.

E2.0 Reason for this protocol

This protocol is intended to protect the security and integrity of the school's data and technology infrastructure, and to make Students aware of their responsibilities when bringing their own equipment in to school.

E3.0 Support

E3.1 The IT Support Team has limited support capabilities for Student devices and, unlike school-owned devices, they cannot undertake to fully support personal devices. The IT Support Team will make reasonable endeavours to support connecting personal devices to the wireless network in the school, but priority will be given to school owned devices.

E3.2 Please note that if support is provided, the IT Support Team may have access to any personal information stored on the device. As part of supporting the device, it may be necessary remove data stored on the device or completely wipe the device if required. The school accepts no responsibility or liability for any loss incurred as a result.

E3.3 The school also reserves the right to remove any applications from a personal device that are considered to be a security risk to the school.

E4.0 Damages

The school is not responsible for any damages, insurance, theft or loss of a personal device on the school site or being transported to or from the school. The school is not responsible for any viruses or malware which infect a personal device while using the school's wireless network.

E5.0 Data responsibility & backups

The school is not responsible for the backup or recovery of data on any personal device used at the school. The responsibility for any personal data remains with the Student.

E6.0 Security

E6.1 Students using a personal device **MUST** ensure the physical security of the device.

E6.2 Some mobile devices contain portable storage devices (PSD) such as flash memory cards that can be used to store data. Students **MUST** ensure the physical security of privately owned PSD's.

E6.3 Jail broken iOS or root broken Android Devices will not be permitted to connect to any school service.

E6.4 Personal devices are subject to the same Acceptable Use Protocol as school-owned devices.

E7.0 Safety

Students **MUST** ensure that devices are safe to use, and are free from electrical faults and damaged casing.

E8.0 Agreement

I acknowledge that I have read and understood the school's Student BYOD Protocol. I accept full responsibility for any device I bring in to school.

PLEASE SIGN AND RETURN THIS FORM TO THE IT SUPPORT OFFICE AT OAKLANDS SCHOOL.

Print Name: _____

Form Group: _____

Signature: _____

Parent/Guardian Signature: _____

Date: _____

Notes: