Support Documents

Workplace Internet, Email and Network Usage Policy

Responsible Officer:	Assistant Directors of Schools
Approval Date:	November 2016
Effective Date:	November 2016

Contents

Catholic Schools Office
DIOCESE OF MAITLAND-NEWCASTLE

School Staff Code of Practice

Purpose

This Code of Practice has been developed for workplace staff in diocesan schools in the Diocese of Maitland-Newcastle and is consistent with the CSO's policy on Workplace Internet, Email and Network Usage Policy (2010). Principals are responsible for ensuring that staff are familiar with the policy and Code of Practice, and operate within the parameters of these documents.

Whilst the Catholic Schools Office/school respects each person's right to privacy, the CSO/school needs to have access to its computer systems and ICT equipment/devices. By using the CSO/school's computer system and/or devices the staff member signing this document recognises that ongoing monitoring occurs on the school's network and the systems administrator (Director, Head of Financial Services, Principal and/or nominee) can access user's mail, data and internet logs.

Mandatory Procedures

Security

- Passwords are only to be made known to authorised staff;
- Passwords for administrative networks are only to be given to authorised staff;
- Students may be given low level access only to educational networks;
- Log workstation off before leaving the building or leaving workstation for extended periods.
- Identifying student information can only be published on the Internet with the written permission of the parent/carer.
- Ensure devices that you join to the network or bring onto CSO or school property or sanctioned school activities do not contain content or are used in any way that are in breach of the Workplace Internet, Email and Network Usage policy

  (NB Device includes but is not limited to laptops, iPods, USB storage devices and mobile phones.)

Supervision

- Student activity on computer networks will be supervised appropriately by staff. Staff will take all reasonable steps to ensure that student activity on networks is in accordance with the School Code of Practice.
- Staff are advised they have responsibility for addressing inappropriate behaviour or activity on social networks, including requirements for mandated reporting.

It is acceptable to

- Facilitate and disseminate knowledge; encourage collaborative projects and resource sharing; foster innovation; build broader infrastructure in support of education and research; foster professional development; undertake administrative functions and any other task which supports the business of the CSO.

It is unacceptable to

Send, forward, attach, upload, transmit, download, link to or store any images, content, links or material that:

- Is, or may be construed to be, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, pornographic, or otherwise offensive.
- Is, or may be construed to be, insulting, vulgar, rude, disruptive, derogatory, harmful or immoral.
- Harasses or promotes hatred or discrimination based on any unlawful grounds against any person.
- Contains any virus, worm, Trojan or other harmful or destructive code.
- Relates to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity.
- Injures the reputation of the Catholic Schools Office and/or school or cause embarrassment to the Catholic Schools Office and/or school.
- Is spam or mass/chain mail.
- Communicates information concerning any password, identifying code, personal identification code or other confidential information;
- Infringes the copyright or other intellectual property rights of another person.
- Involves gaming, wagering or betting.
- Is personal business activity for financial gain or commercial purposes
- Is defined as illegal activities under the Australian Commonwealth Government Telecommunications Act 1997 or Crimes Act, NSW, 1900 Section 578C, Crimes Amendment Act (Child Pornography) NSW Schedule 1.
- use social media such as Facebook, Twitter etc. as a platform for learning activities with students.
- accept students as 'friends' on their own private social media sites or interact with students on their social media sites
- discuss students or coworkers or publicly criticise school policies or personnel on social media sites.
- post images that include students on private social media sites without explicit permission from a student's parent or guardian.

I understand that should I breach these requirements, I may be subject to formal disciplinary and/or legal proceedings.

Employees of the Diocese of Maitland-Newcastle Catholic Schools Office are required to sign the following declaration to enable access/or continue access to the Internet, Email and Network services via the CSO Local and/or Wide Area Network.

I declare I have read and understood the Diocese of Maitland-Newcastle CSO's Workplace Internet, Email and Network Usage Policy (2013) and the accompanying Code of Practice.

School	
Surname	
Given Name	
Position	

Signature ..... **Date**.....

OFFICE USE ONLY

The original declaration is to be retained at the school

Principal ..... **Date**.....

Catholic Schools Office
DIOCESE OF MAITLAND-NEWCASTLE

CSO & Non-school Workplace Staff Code of Practice

Purpose

This Code of Practice has been developed for all CSO and other non-school workplace staff and is consistent with the CSO's policy on Workplace Internet, Email and Network Usage Policy (2009). Heads of Service are responsible for ensuring that staff are familiar with the policy and Code of Practice, and operate within the parameters of these documents. This includes the supervision of students who may be utilising facilities within the CSO's offices.

Whilst the Catholic Schools Office respects each person's right to privacy, the CSO needs to have access to its computer systems and ICT equipment/devices. By using the CSO or school computer system and/or devices the staff member signing this document recognises that ongoing monitoring occurs on the school's network and the systems administrator (Director, Head of Financial Services and/or nominee) can access user's mail, data and internet logs.

Mandatory Procedures

Security

- Passwords are only to be made known to authorised staff;
- Passwords for administrative networks are only to be given to authorised staff;
- Students may be given low level access only to educational networks;
- Log workstation off before leaving the building or leaving workstation for extended periods.
- Identifying student information can only be published on the Internet with the written permission of the parent/carer.
- Ensure devices that you join to the network or bring onto CSO or school property or sanctioned school activities do not contain content or are used in any way that are in breach of the Workplace Internet, Email and Network Usage policy

(NB Device includes but is not limited to laptops, iPods, USB storage devices and mobile phones.)

Supervision

- Student activity on computer networks will be supervised appropriately by staff. Staff will take all reasonable steps to ensure that student activity on networks is in accordance with the School Code of Practice.

It is acceptable to

- Facilitate and disseminate knowledge; encourage collaborative projects and resource sharing; foster innovation; build broader infrastructure in support of education and research; foster professional development; undertake administrative functions and any other task which supports the business of the CSO.

It is unacceptable to

- send, forward, attach, upload, transmit, download, link to or store any images, content, links or material that:
- Is, or may be construed to be, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, pornographic, or otherwise offensive.
- Is, or may be construed to be, insulting, vulgar, rude, disruptive, derogatory, harmful or immoral.
- Harasses or promotes hatred or discrimination based on any unlawful grounds against any person.
- Contains any virus, worm, Trojan or other harmful or destructive code.

- Relates to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity.
- Injures the reputation of the Catholic Schools Office and/or school or cause embarrassment to the Catholic Schools Office and/or school.
- Is spam or mass/chain mail.
- Communicates information concerning any password, identifying code, personal identification code or other confidential information;
- Infringes the copyright or other intellectual property rights of another person.
- Involves gaming, wagering or betting.
- Is personal business activity for financial gain or commercial purposes
- Is defined as illegal activities under the Australian Commonwealth Government Telecommunications Act 1997 or Crimes Act, NSW, 1900 Section 578C, Crimes Amendment Act (Child Pornography) NSW Schedule 1.
- Discuss students or co-workers or publicly criticise school policies or personnel on social media sites.
- Post images that include students on private social media sites without explicit permission from a student's parent or guardian.

I understand that should I breach these requirements, I may be subject to formal disciplinary and/or legal proceedings.

Employees of the Diocese of Maitland-Newcastle Catholic Schools Office are required to sign the following declaration to enable access/or continue access to the Internet, Email and Network services via the CSO Local and/or Wide Area Network.

I declare I have read and understood the Diocese of Maitland-Newcastle CSO's Workplace Internet, Email and Network Usage Policy (2013) and the accompanying Code of Practice.

Service Area	
Surname	
Given Name	
Position	

Signature ..... **Date**.....

OFFICE USE ONLY

The original declaration is to be retained at the CSO by the Head of Financial Services

Head of Service ..... **Date**.....

Instructions for students, parents*, caregivers, legal guardians

This document contains this cover page and three sections:

Section A: Introduction

Section B: Cybersafety Rules for Primary Students

Section C: Cybersafety Use Agreement Form.

---

1. **Please read sections A and B carefully.**
2. **Discuss the cybersafety rules with your child.**
3. **Sign the user agreement form (Section C) and return that page to the school office.**
4. **Please keep Sections A and B for future reference.**

Important terms used in this document:

(a) *The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies'*

(b) ***'Cybersafety'** refers to the safe use of the Internet and ICT equipment/devices, including mobile phones*

(c) ***'School ICT'** refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below*

(d) *The term **'ICT equipment'** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, ICT device as they come into use*

(e) *'**Objectionable**' in this agreement means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment.*

** The term 'parent' used throughout this document also refers to legal guardians and caregivers.*

Section A: Introduction

The school's computer network, Internet access facilities, computers and other school ICT equipment bring great benefits to the teaching and learning programs and to the effective operation of the school. The use of the school's ICT equipment are for educational purposes appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on *or* off the school site. Parents need to note that while our school has rigorous cybersafety practices in place, it is not possible to completely eliminate the risk of exposure to inappropriate online content.

The school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including email. You should be aware that general internet browsing by your child from home or other locations other than school are not monitored or filtered by the school.

The school may audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit.

All students will be issued with a user agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment.

Section B: Cybersafety Rules for Primary Students

1. I cannot use school ICT equipment until my parent(s) and I have signed my Cybersafety User Agreement form and the completed form has been returned to school.

2. I can only use the computers and other school ICT equipment for my schoolwork.

3. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.

4. I will log on only with the user name that has been provided by the school. I will not allow anyone else to use my user name and I will not tell anyone else my password.

5. I can only go online or access the Internet at school when a teacher gives permission and an adult is present.

6. I understand that I must not, at any time, use the Internet, social media, email, mobile phones or any ICT equipment to be mean, rude, offensive, or to bully, harass, or in any way harm anyone else connected to our school, or the school itself, even if it is meant as a 'joke'.

7. While at school, I will not:
   - Attempt to search for things online I know are not acceptable at our school. This could include anything that is rude or violent or uses unacceptable language such as swearing
   - Make any attempt to get around, or bypass, security, monitoring and filtering that is in place at our school.

8. If I find anything mean or rude or things I know are not acceptable at our school on any ICT, I will:

   Not show others

   Exit the program or turn off the screen

   and Get a teacher straight away.

9. I understand that I must not download or copy any files such as music, videos, games or programs without the permission of a teacher. This is to ensure we are following copyright laws.

10. I must have permission from school before I bring any ICT equipment/device from home. This includes things like mobile phones, iPods, games, cameras, and USB drives.

11. I will not connect any device (such as a USB drive, camera or phone) to school ICT network or run any software, without a teacher's permission. This includes all wireless technologies.

12. The school cybersafety rules apply to any ICT equipment brought to school like a mobile phone or ipod and I am responsible for the material on these devices. I also understand that the school can view the contents stored on these devices.

13. I will ask my teacher's permission before giving out any personal information online. I will also get permission from any other person involved.

Personal Information includes:

a) Name

b) Address

c) Email address

d) Phone numbers

e) Photos.

14. I will respect all school ICT equipment and will treat all ICT equipment with care. This includes:

- Not intentionally disrupting the smooth running of any school ICT systems
- Not attempting to gain unauthorised access to any system
- Following all school cybersafety rules, and not joining in if other students choose to be irresponsible with ICT
- Reporting any breakages/damage to a staff member.

15. I understand that if I break these rules, the school may need to inform my parents. In serious cases the school may take disciplinary action against me. I also understand that my family may be charged for repair costs.

Section C: Primary School Cybersafety User Agreement

Schools and the CSO will be doing their best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or school ICT equipment and devices at school, or at school-related activities. Working progressively with students and their families, teachers will encourage and develop an understanding of the importance of cybersafety. This includes providing children with strategies to keep themselves safe in cyberspace and attending to enquiries from parents or students about cybersafety issues.

We will respond to any breaches in an appropriate manner as per the CSO Workplace Internet, Email and Network Usage Policy document.

To the student/parent/caregiver/legal guardian, please:

1. Read this page carefully to ensure that you understand your responsibilities under this agreement
2. Sign the appropriate section on this form
3. Detach and return this form to the school office
4. Keep the document for future reference, as well as the copy of this signed page which the school will provide.

Responsibilities include:

- Reading this cybersafety user agreement document
- Discussing the information with my child and explain why it is important
- Returning the signed agreement to the school
- Supporting the school's cybersafety program by encouraging my child to follow the cybersafety rules, and to always ask the teacher if they are unsure about any use of ICT
- Contacting the principal to discuss any questions I might have about cybersafety and/or this user Agreement.

Please detach and return this section to school.

I have read this cybersafety user agreement and I am aware of the school's initiatives to maintain a cybersafe learning environment, including my child's responsibilities.

Name of student: ..... Class: .....

Signature of Student: .....

Name of parent/caregiver/legal guardian: .....

Signature or parent:..... Date: .....

Please note: This agreement for your child will remain in force as long as he/she is enrolled at this school. If it becomes necessary to add/amend any information or rule, parents will be advised in writing.

Instructions for students

This document contains this cover page and three sections:

Section A: Introduction

Section B: Cybersafety Rules for Secondary Students

Section C: Cybersafety Use Agreement Form.

---

1. **Please read sections A and B carefully. If there are any points you would like to discuss with the school, let the school office know as soon as possible.**
2. **Discuss the cybersafety rules with your child.**
3. **Sign the user agreement form (Section C) and return that page to the school office.**
4. **Please keep Sections A and B for future reference.**

Important terms used in this document:

*(f) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies'*

*(g) **'Cybersafety'** refers to the safe use of the Internet and ICT equipment/devices, including mobile phones*

*(h) **'School ICT'** refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below*

*(i) The term **'ICT equipment'** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, ICT device as they come into use*

*(j) '**Objectionable**' in this agreement means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment.*

** The term 'parent' used throughout this document also refers to legal guardians and caregivers.*

Section A: Introduction

The school's computer network, Internet access facilities, computers and other school ICT equipment bring great benefits to the teaching and learning programs and to the effective operation of the school. The use of the school's ICT equipment are for educational purposes appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on *or* off the school site. Parents need to note that while our school has rigorous cybersafety practices in place, it is not possible to completely eliminate the risk of exposure to inappropriate online content.

The school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including email. You should be aware that general internet browsing by your child from home or other locations other than school are not monitored or filtered by the school.

The school may audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit.

All students will be issued with a user agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment.

Section B: Cybersafety Rules for Secondary Students

1. I cannot use school ICT equipment until my parent(s) and I have signed my Cybersafety User Agreement form and the completed form has been returned to school.

2. I will log on to school ICT with the user name the school has issued me with. I will not allow anyone else to use my user name. I will not tell anyone else my password.

3. While at school or a school-related activity, I will not have any involvement with any ICT material or activity which might put myself or anyone else at risk (e.g. bullying or harassing).

4. I understand that I must not at any time use ICT including social media (e.g. Facebook, Twitter etc.) to upset, offend, harass, bully or threaten or in any way harm anyone connected to the school or the school itself, even if it is meant as a joke.

5. I understand that the rules in this use agreement also apply to mobile phones. I will only use my mobile phone(s) at the times that I am permitted to during the school day.

6. I understand that I can only use the Internet at school when a teacher gives permission and there is staff supervision.

7. While at school, I will not:
    a. Access, or attempt to access, inappropriate, age restricted, or objectionable material.
    b. Download, save or distribute such material by copying, storing, printing or showing it to other people.
    c. Make any attempt to bypass security, monitoring and filtering that is in place at school. This includes but is not limited to the use of Internet proxy anonymisers.

8. If I accidentally access inappropriate material, I will:

    a) Not show others

    b) Turn off the screen or minimise the window and

    c) Report the incident to a teacher immediately

9. I understand that I must not download any files such as music, videos, games or programs without the permission of a teacher. This makes sure the school complies with the Copyright Act 2006. I also understand that anyone who infringes copyright may be personally liable under this law.

10. I understand that these rules apply to any privately owned ICT equipment (such as a laptop, mobile phone, USB drive) I bring to school or a school-related activity. Any images or material on such equipment must be appropriate to the school environment. I also understand that the school can view the contents stored on these devices when brought to school or a school activity.

11. I will not connect any device (such as a USB drive, camera or phone) to, or attempt to run any software on, school ICT without a teacher's permission. This includes all wireless technologies.

12. I will ask a teacher's permission before giving out any personal information (including photos) online about myself or any other person. I will also get permission from any other person involved. Personal information includes name, address, email address, phone numbers, and photos.

13. I will respect all ICT systems in use at school and treat all ICT equipment with care. This includes:

    - Not intentionally disrupting the smooth running of any school ICT systems
    - Not attempting to gain unauthorised access to any system
    - Following all school cybersafety rules, and not joining in if other students choose to be irresponsible with ICT
    - Reporting any breakages/damage to a staff member.

15. I understand that the school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including email.

16. I understand that the school may audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including email.

17. I understand that if I break these rules, the school may inform my parent(s). In serious cases the school may take disciplinary action against me. I also understand that my family may be charged for repair costs. If illegal material or activities are involved, it may be necessary for the school to inform the police.

Section C: Secondary School Cybersafety User Agreement

Schools and the CSO will be doing their best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or school ICT equipment and devices at school, or at school-related activities. Working progressively with students and their families, teachers will encourage and develop an understanding of the importance of cybersafety. This includes providing children with strategies to keep themselves safe in cyberspace and attending to enquiries from parents or students about cybersafety issues.

We will respond to any breaches in an appropriate manner as per the CSO Workplace Internet, Email and Network Usage Policy document.

To the student/parent/caregiver/legal guardian, please:

1. Read this page carefully to ensure that you understand your responsibilities under this agreement
2. Sign the appropriate section on this form
3. Detach and return this form to the school office
4. Keep the document for future reference, as well as the copy of this signed page which the school will provide.

Student responsibilities include:

- Reading this cybersafety use agreement carefully and discussing the agreement with my parents.
- Following the cybersafety rules and instructions whenever I use the school's ICT
- Following the cybersafety rules whenever I use privately-owned ICT on the school site or at any school-related activity, regardless of its location
- Avoiding any involvement with material or activities which could put at risk my own safety, or the privacy, safety or security of the school or other members of the school community
- Taking proper care of school ICT. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, my family may be responsible for the cost of repairs or replacement
- Keep this document somewhere safe so I can refer to it in the future
- Asking the school's staff if I am not sure about anything to do with this agreement.

Please detach and return this section to school.

I have read this cybersafety user agreement and I am aware of the school's initiatives to maintain a cybersafe learning environment, including my child's responsibilities.

Name of student: ..... Tutor Group/Roll Class: .....

Signature of Student: .....

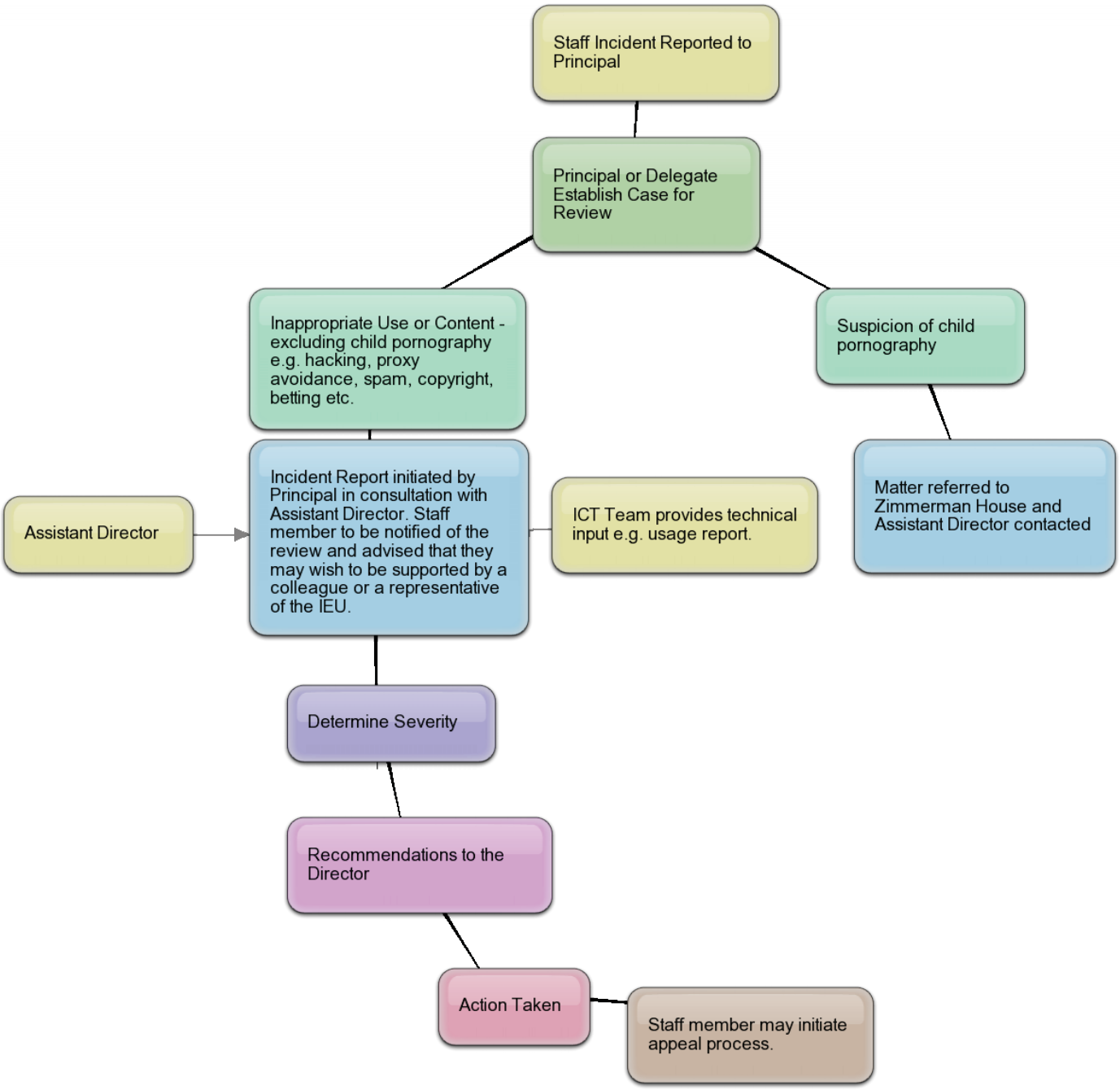
Name of parent/caregiver/legal guardian: .....

Signature or parent:..... Date:.....

Please note: This agreement for your child will remain in force as long as he/she is enrolled at this school. If it becomes necessary to add/amend any information or rule, parents will be advised in writing.

School Staff Incident Report Flowchart

Workplace Internet, Email and Network Usage



Catholic Schools Office
DIOCESE OF MAITLAND-NEWCASTLE

School Staff Incident Report

Workplace Internet, Email and Network Usage

School: ..... Date:.....

Staff Name: .....

REVIEW CATEGORY: (TICK CATEGORY)

Inappropriate Use ☐ e.g. Network hacking, bullying, proxy avoidance, spam, copyright etc.

Inappropriate Content ☐ e.g. Social media, pornographic material etc.

If there is suspicion of child pornography the Principal MUST immediately make contact with Zimmerman Services to investigate and the relevant Assistant Director. DON'T copy, view or delete any content.

REASON FOR REVIEW:

.....

.....

.....

REVIEW UNDERTAKEN BY:

Name:..... Role:.....

Name:..... Role:.....

Name:..... Role:.....

The relevant Assistant Director been consulted: ☐ Name:.....

The CSO ICT team has been involved: ☐ Name:.....

The staff member has been notified and they have been advised to consult with a colleague or representative of the IEU. ☐

Degree of Severity of the incident: Low ☐ Medium ☐ High ☐

RECOMMENDATIONS: To Whom:.....

.....

.....

.....

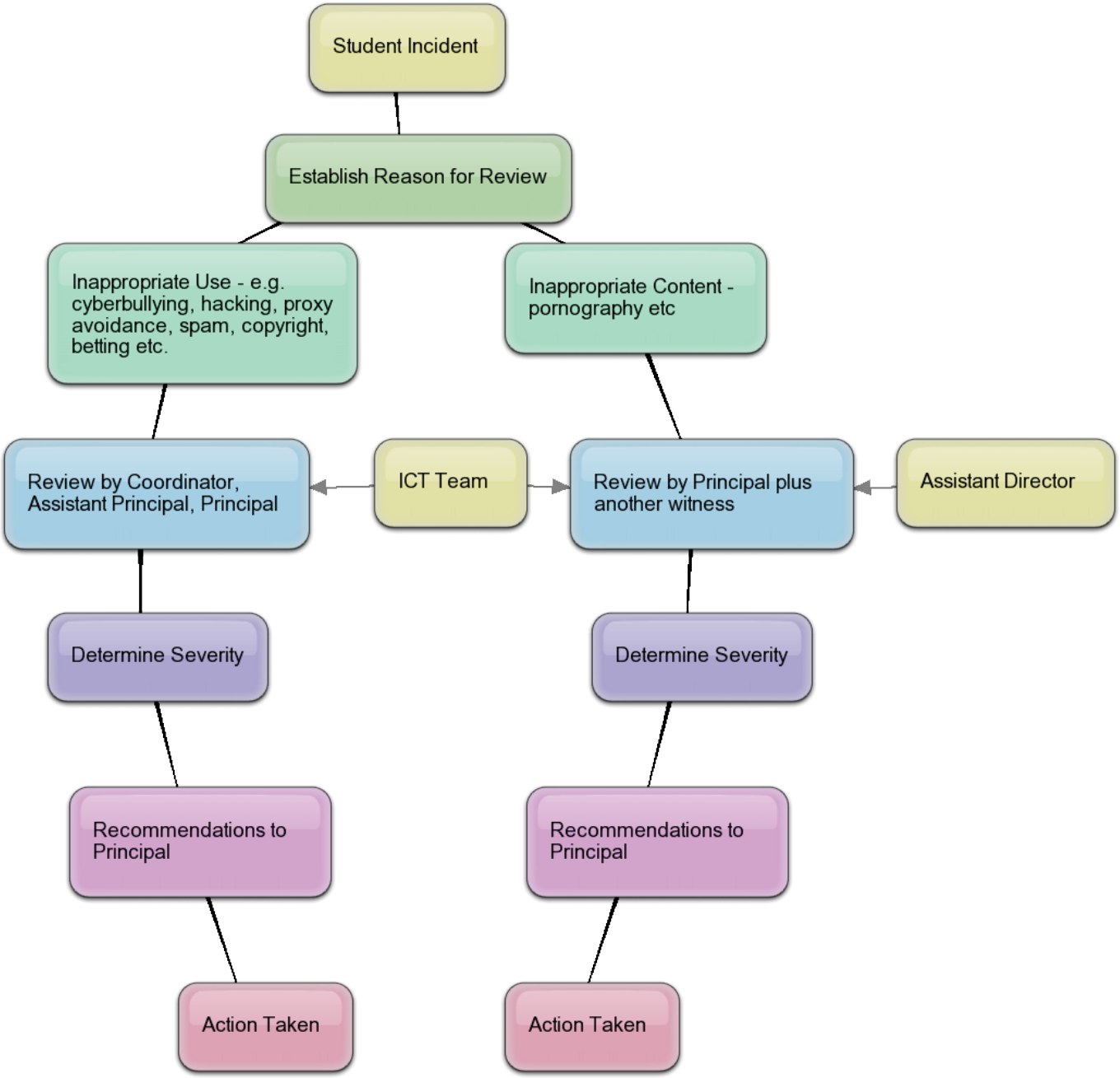
Action Taken: ..... By Whom:.....

Signed: ..... Date:.....

Catholic Schools Office
DIOCESE OF MAITLAND-NEWCASTLE

Student Incident Report Flowchart

Workplace Internet, Email and Network Usage



NEALS

Catholic Schools Office
DIOCESE OF MAITLAND-NEWCASTLE

Student Incident Report

Workplace Internet, Email and Network Usage

School: ..... Date:.....

Student Name: .....

REVIEW CATEGORY: (TICK CATEGORY)

Inappropriate Use ☐ e.g. Network hacking, proxy avoidance, spam, copyright etc.

Inappropriate Content ☐ e.g. Social media, pornographic material etc.

REASON FOR REVIEW:

.....

.....

.....

REVIEW UNDERTAKEN BY:

Name:..... Role:.....

Name:..... Role:.....

Name:..... Role:.....

The relevant Assistant Director been consulted: ☐ Name:.....

The CSO ICT team has been involved: ☐ Name:.....

The staff member has been notified and they have been advised to consult with a colleague or representative of the IEU. ☐

Degree of Severity of the incident: Low ☐ Medium ☐ High ☐

RECOMMENDATIONS: To Whom:.....

.....

.....

.....

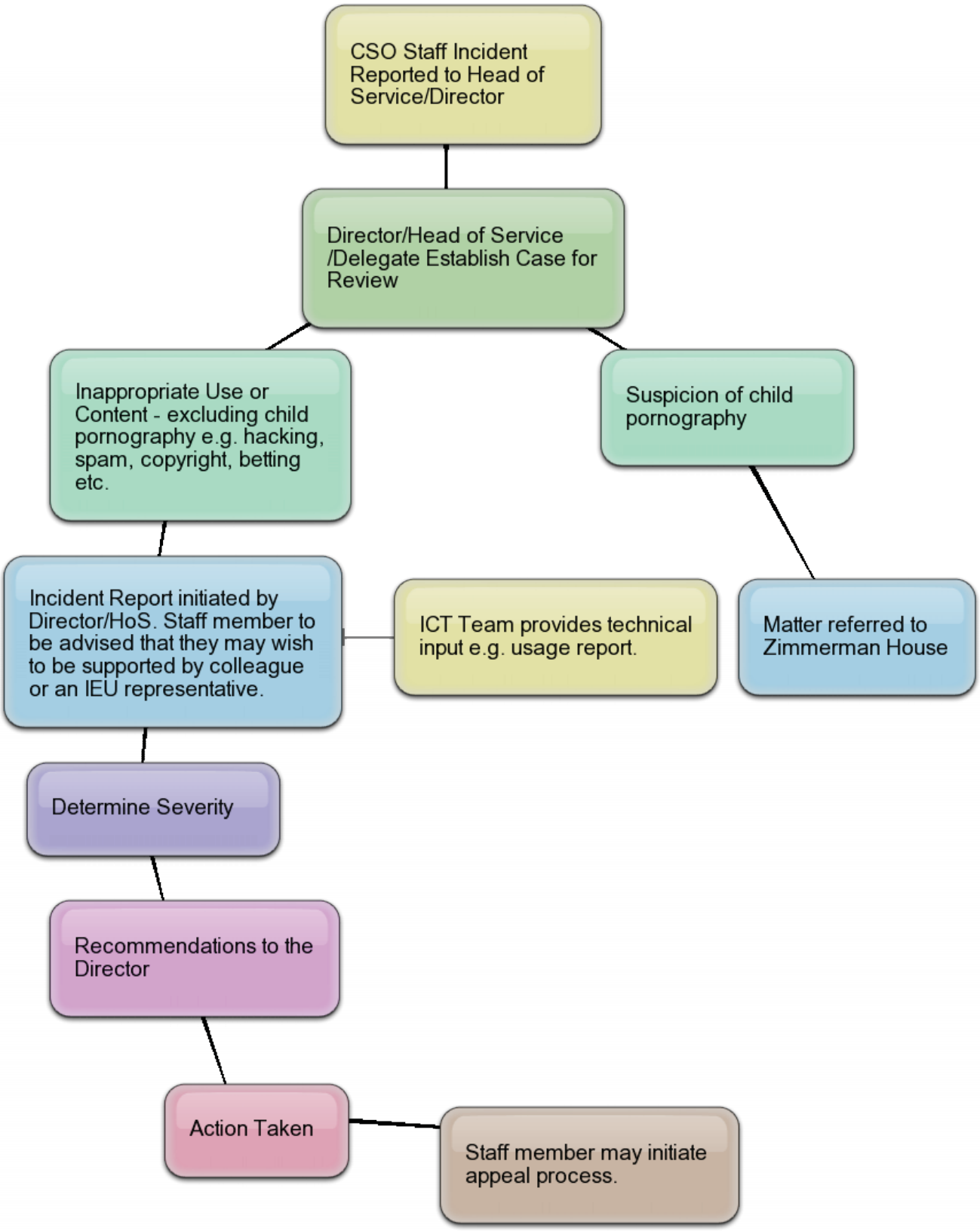
Action Taken: ..... By Whom:.....

Signed: ..... Date:.....

NEALS

CSO Staff Incident Report Flowchart

Workplace Internet, Email and Network Usage



CSO Staff Incident Report

Workplace Internet, Email and Network Usage

CSO Service Area: ..... Date:.....

Staff Name: .....

REVIEW CATEGORY: (TICK CATEGORY)

Inappropriate Use ☐ e.g. Network hacking, proxy avoidance, spam, copyright etc.

Inappropriate Content ☐ e.g. Social media, pornographic material etc.

If there is suspicion of child pornography the Principal MUST immediately contact Zimmerman Services to investigate and the relevant Assistant Director. DON'T copy, view or delete any content.

REASON FOR REVIEW:

.....

.....

.....

REVIEW UNDERTAKEN BY:

Name:..... Role:.....

Name:..... Role:.....

Name:..... Role:.....

Relevant Head of Service/ Director been consulted: ☐ Name:.....

The CSO ICT team has been involved: ☐ Name:.....

The staff member has been notified and they have been advised to consult with a colleague or representative of the IEU. ☐

Degree of Severity of the incident: Low ☐ Medium ☐ High ☐

RECOMMENDATIONS: To Whom:.....

.....

.....

.....

Action Taken: ..... By Whom:.....

Signed: ..... Date:.....

Parent Declaration for Social Media Involvement

Our school social media pages are available to all, providing families with the latest information regarding happenings at our school. The pages allow the school to give quick reminders of events and update any last minute changes when a note to the whole school is not possible. The school can also share some of the achievements or highlights of school events.

It is important to note that this will not replace any of the school's existing forms of communication so there is no disadvantage in not having access to online social media pages. It will just be another means of communication for anyone who is interested.

In line with the CSO's Social Media Acceptable Community Use and Content Policy parents are asked to follow these important guidelines when using the school's official social media pages.

Please read these carefully.

- The school's social media pages are designed to give up-to-date information to members of the school community. It is **not** a space to vent frustrations or name and shame anyone in our community. Parents wishing to make a complaint should refer to the CSO's Complaints and Grievances Resolution Policy (2013) and the accompanying support documents.
- Parents are asked **not to share** information, photos, videos, etc. of any individual other than themselves without clearly expressed permission prior to publication.

Parent Declaration

I agree to abide by the above guidelines in regards to my use of the school's social media pages.

Name:..... Date:.....

Signature: .....