



LUX MUNDI

LIGHT OF THE WORLD ~ CATHOLIC ACADEMY TRUST

Online Safety Policy 2024-25

CARDINAL POLE CATHOLIC SCHOOL

Status: Public

APPROVED BY THE LOCAL GOVERNING BODY ON: 4th December 2024

CHAIR OF GOVERNOR'S SIGNATURE:.....
Madhubu

Contents

Cardinal Pole School Vision.....	3
Mission Statement.....	3
Policy Statement.....	3
Role & Responsibilities.....	4
Reporting Concerns.....	5
Technology.....	6
Safe Use.....	6
Acceptable use Policy (staff).....	8
Acceptable Use Policy (students).....	9
Inappropriate Activity Flowchart.....	10
Illegal Activity Flowchart.....	11

Cardinal Pole School Vision

Cardinal Pole Catholic School is a learning community for all based upon partnership and respect. It is a strong and vibrant place which recognizes the importance and individual needs of every pupil and member of staff. Praise and encouragement is vital in creating a climate of learning and high expectations supported by teaching of the highest quality. The school is full of confident, creative and fulfilled young people and staff. They are celebrated as individuals – unique creations of God – who deserve our support, love and trust as they begin the great journey of life.

Mission Statement

Cardinal Pole Catholic School is a community of **service** guiding young people on a path to **opportunity, aspiration, and reward**, founded on Catholic values. We serve our students through bespoke interventions that meets the needs of all. This is shared with all stakeholders, to empower our community to become “Lovers of Reading”. Cardinal Pole Catholic School is committed to providing a range of opportunities for staff and students to become lifelong lovers of reading through workshops, authors visits, whole school events and programmes. We are a community of aspirant writers where talent is nurtured or flourish by expert and experienced staff, authors, and other professionals. We reward our literate learners by celebrating their successes, progress, achievements in all areas of literacy and beyond.

Policy Statement

For clarity, the Online Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents

Safeguarding is a serious matter; at Cardinal Pole Catholic School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as Online Safety is an area that is constantly evolving and as such this policy will be reviewed every three years or in response to an Online Safety incident, whichever is sooner.

The primary 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.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Cardinal Pole Catholic School website; upon review all members of staff will sign as read and understood both the Online Safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Executive Headteacher: Mr Adam Hall Signed:

Chair of Governors: Justin Madubuko Signed:

Review Date: Next Review:

(This policy is to be read in conjunction with the School Safeguarding Policy and Keeping Children Safe in Education 2024)

Policy Governance (Roles & Responsibilities)

Governing Body

The Governing Body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy every three years and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Online Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
 - Chair the Online Safety Committee

Executive Headteacher

Reporting to the Governing Body, the Executive Headteacher has overall responsibility for Online Safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Officer (or more than one), as indicated below.

The Executive Headteacher will ensure that:

- Online 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 Online Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All Online Safety incidents are dealt with promptly and appropriately.

Online Safety Officer

The day-to-day duty of Online Safety Officer is devolved to Mr P McEvoy as part of his role as the Safeguarding Lead.

The Online 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 Executive Headteacher.
- Advise the Executive Headteacher, Governing Body on all Online Safety matters.
- Engage with parents and the school community on Online 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 Online Safety incident log on CPOMS; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical Online 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 Online Safety measures, i.e. internet filtering reporting function; liaise with the Executive Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
 - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
 - Any Online Safety technical solutions such as Internet filtering are operating correctly.
 - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online Safety officer and Executive Headteacher.
 - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.
 - The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

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 Online Safety incident is reported to the Online Safety Officer (and a Blue Form completed) or in his/her absence to the Executive Headteacher. If you are unsure the matter is to be raised with the Online Safety Officer or the Executive Headteacher to make a decision.
- The reporting flowcharts contained within this Online Safety policy are fully understood.

All Students

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.

Online 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.

Parents and Carers

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 and school newsletters the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to 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.

Reporting Concerns

If there are concerns about online activity involving a child, the concern must be reported to the DSL Team using a **Blue Form** (available from the office and staff rooms). If the concern is urgent it must be reported to one of the DSLs immediately.

Safeguarding Officer:	Peter McEvoy
Designated Safeguarding Lead/Head of School:	Alex O'Donoghue
Deputy Safeguarding Lead:	Cynthia John
Deputy Safeguarding Lead:	Tom Read

Technology

Cardinal Pole Catholic School uses a range of devices including PC's, laptops, Apple Macs and tablets. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use software (RM Safety Net) that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate 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 ICT Coordinator, Online 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.

Internet Monitoring – we use software (Smoothwall) that monitors users' (staff and students) activity on the school network and alerts the DSL/Safeguarding to any inappropriate or worrying behavior. This is in place whether the user is in school or off site.

Email Filtering – we use software that prevents any infected email to be sent from the school or to be 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.

Encryption – All school devices that hold personal data (as defined by GDPR 2018) 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 keydrives) is to be brought to the attention of the Executive Headteacher immediately. The Executive Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

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 termly basis or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed.

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 such as key drives are to be scanned for viruses before use.

Safe Use

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

Email – 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.

Social Networking – there are many social networking services available; Cardinal Pole 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 Cardinal Pole Catholic School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Online Safety Officer who will advise the Executive 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).
- You Tube Channel

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.

In addition, the following is to be strictly adhered to:

- Permission slips 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).

Notice and take down policy – should it come to the school’s 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.

Incidents - Any Online Safety incident including online bullying, sexting and peer on peer abuse is to be brought to the immediate attention of the Online Safety Officer, or in his/her absence the Executive Headteacher. The Online Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - 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, Cardinal Pole Catholic School will have an annual programme of training which is suitable to the audience.

Online 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.

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

The Online Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Executive 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 Executive Headteacher for further CPD.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the Online Safety Policy. Once you have read and understood both you must sign this policy sheet

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an Online Safety incident, reported to the Online Safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the Online Safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become “friends” with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pen drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Executive Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the Online Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the RM Helpdesk as soon as it is practical to do so, along with the name of the virus (if known). Malware is a category of malicious code that includes viruses, worms, and Trojan horses.

Online Safety – like health and safety, Online Safety is the responsibility of everyone to everyone. As such you will promote positive Online Safety messages in all use of ICT whether you are with other members of staff or with students.

NAME:

SIGNATURE:

DATE:

Acceptable Use Policy – Students

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people’s work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people’s usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated and will not engage in any form of online/social media bullying.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there may be formal sanctions including exclusion and my parents will be told.

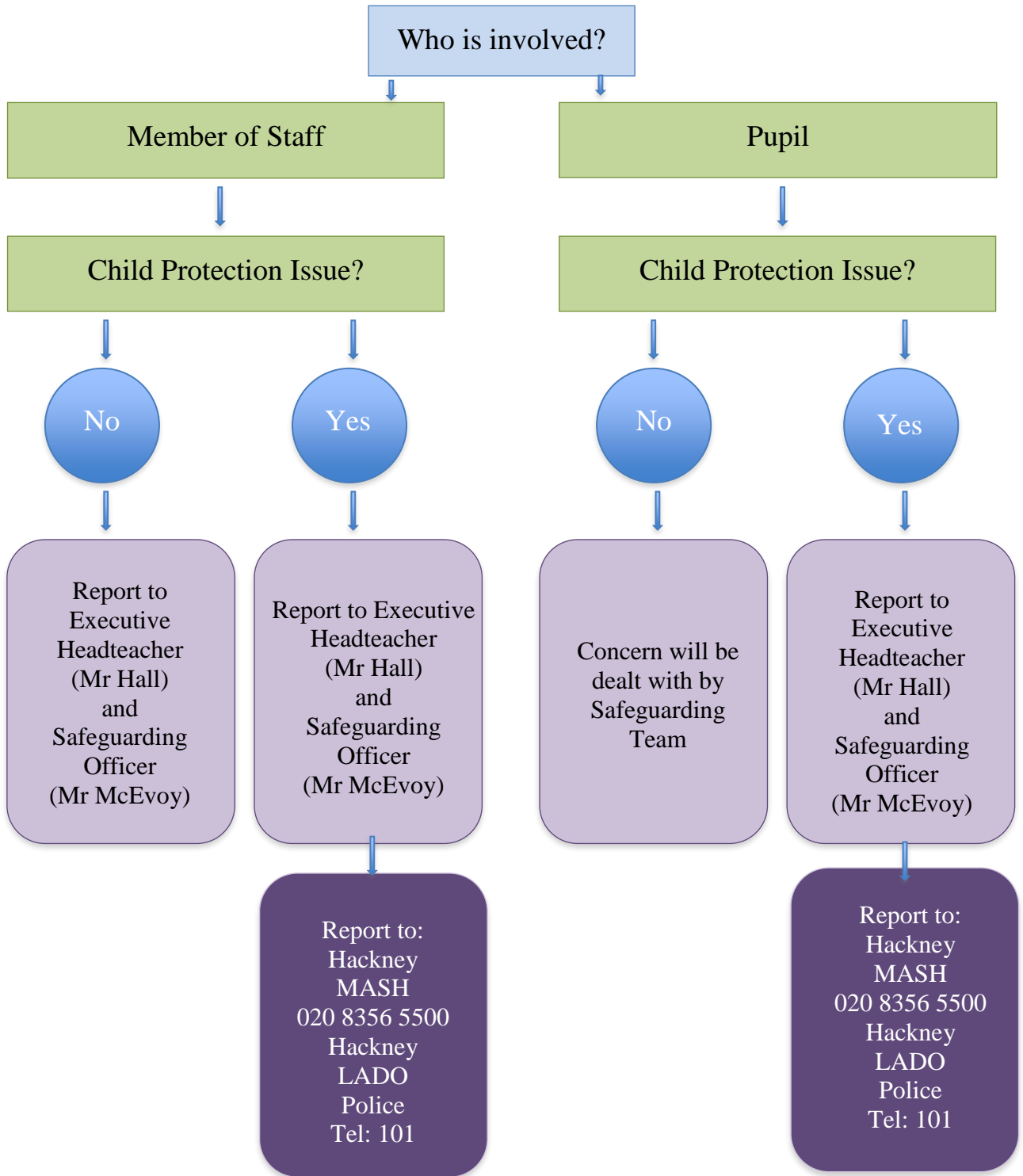
Signed (Parent):

Signed (Student):

Date:

Inappropriate Activity Flowchart

A concern is identified & Blue Form Completed.
If concern is urgent it must be shared with DSL immediately.



If you are in any doubt, consult the Executive Headteacher, or any member of The Safeguarding Team

Illegal Activity Flowchart

Any suspected illegal activity must be reported to the Executive Headteacher and Safeguarding Officer immediately.

