ON LINE SAFETY POLICY

Approved By Governors

Committee Pastoral Committee

Review Date 20th June 2018

Prepared by: Mrs J Ackroyd

Signed Chair of Governors 

Due for Renewal 19th June 2019

All of our polices are directly derived from our Mission Statement:

"Our Lady & St John Catholic College aims to be a caring Catholic community centred on Christ, so as to fully develop the gifts and talents of each person in order to love and serve God, others and themselves."

Purpose

Safeguarding is a serious matter. At Our Lady & St John 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.

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 pupil or liability to the school.

This policy is available for anybody to read on the school's website.

All staff will sign the Staff Acceptable Use Agreement.

All pupils and their parents/carers will sign the Acceptable Use Agreement.

For quality and assurance purposes, procedures will be reviewed in line with policy, at the termly e-safety committee meetings.

Definitions:

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils 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 – pupils, all staff, governing body, parents.

Policy Governance (Roles & Responsibilities)

GOVERNING BODY

The governing body will:

Review the policy at least annually 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 and ensures the policy facilitates effective management of incidents.

Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:

- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the Headteacher with regards to training, identified risks and any incidents.

HEADTEACHER

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within the school. The day-to-day management of this will be delegated to the Safeguarding Lead/DSL.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, staff, Senior Leadership Team, Governing Body and parents.
- The Safeguarding Lead/DSL has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

SAFEGUARDING LEAD/DESIGNATED SAFEGUARDING LEAD (DSL)

The school's Safeguarding Lead/DSL will act as the E-Safety Officer who will:

- Lead the e-safety committee
- Keep up to date with the latest risks to children whilst using technology. This includes the risks associated with radicalisation, Child Sexual Exploitation (CSE) and Sexting.
- Familiarise him/herself with the latest research and available resources for school and home use.
- Review the policy regularly and bring any matters of concern to the attention of the Headteacher.
- Advise the Headteacher and Governing Body on all e-safety matters.
- Recommend a programme of training and awareness for the school year, to the Headteacher and responsible Governor, for consideration and planning.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the Local Authority, ICT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log which will be located on a secure shared folder, accessed by the Safeguarding Lead/DSL, ICT Services and Assistant Head – Behaviour and Attendance.
- Ensure any technical e-safety practices in school (e.g. Internet filtering software, behavior 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.

ICT TECHNICAL SUPPORT STAFF

ICT Technical Support Staff, under the direction of the ICT Network Manager, are responsible for ensuring that:

- The ICT technical infrastructure is secure; this will include at a minimum that:
  - Adequate backups are made of the network.
  - Anti-virus software 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 e-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 Safeguarding Lead/DSL and Headteacher.
  - Passwords are applied correctly to all users regardless of age.
  - The ICT System Administrator's password is changed on a monthly (30 day) basis.
  - ***There is a system in place to remove and amend access permissions for changes to staff duties or terminations; when a member of staff leaves, permissions are to be deactivated and access to ICT systems removed.***

ALL STAFF

All staff are to ensure that:

- All details within this policy are understood.
- All opportunities are exploited to promote safe behaviour on-line.
- Whenever ICT is used in the school, there are positive messages about the safe use of technology and risks as part of pupils' learning.
- Safe behaviour regarding social networking is promoted.
- Any e-safety incident is reported to the Safeguarding Lead/DSL (and an e-Safety Incident report is made), or in his/her absence to the Headteacher.
- The reporting procedure is fully understood. Any e-safety incident should be brought to the immediate attention of the Safeguarding Lead/DSL, or in his/her absence the Headteacher. (**Appendix 1)**
- They participate in relevant training to keep up to date with advancing technology and the potential dangers associated with it; particular vigilance will be exercised in relation to sexting. **(Appendix 2)**

All Staff will:

- Sign the Acceptable Use Agreement. **(Appendix 3)**
- Report any inappropriate activity to the DSL.
- Undertake relevant training as directed by the Headteacher.

Staff should be mindful that many children have unlimited and unrestricted access to the Internet via 3G and 4G in particular, on their personal mobile digital devices. Messages regarding safe use should be promoted whenever possible. The behaviour for learning policy should be followed relating to the restrictions around the use of personal mobile devices in school.

ALL PUPILS

All pupils will sign the Acceptable Use Agreement. (**Appendix 4)**

E-Safety is embedded into our curriculum. The boundaries of use of ICT equipment and services in school will be made clear to pupils. Pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be made aware of how they can report areas of concern whilst at school or outside of school. Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour for learning policy/flow chart. (Appendix 3).

Sexting incidents will be dealt with in accordance with UKCCIS guidance.

PARENTS AND CARERS

School needs to have rules in place to ensure that pupils can be properly safeguarded. As such, parents/carers are asked to sign the Acceptable Use agreement before any access can be granted to school ICT equipment or services.

The school will support parents in keeping their children safe on line by publishing information on the school's web-site.

Parents are advised to monitor their child's Internet activity when using their own personal computers/digital technology.

All parents/carers will counter-sign the Pupil Acceptable Use Agreement. **(Appendix 4)**

E-SAFETY COMMITTEE

The Our Lady & St John e-safety committee has the following members:

- Safeguarding/e-safety Governor
- Pupil Voice Representative
- Safeguarding Lead
- ICT Network Manager
- SLT member responsible for behaviour

The e-safety committee will meet on a termly basis and has responsibility for:

- Advising on changes to the e-safety policy.
- Establishing the effectiveness (or not) of e-safety training and awareness in the school.
- Recommending any necessary further action relating to e-safety training and awareness.
- Reviewing policy and practice.

Standing Agenda Items:

- Review of policy and practice (annually)
- Review of roles and responsibilities (annually)
- Review of updates in legislation
- Termly review of incident log
- Termly review of Acceptable use signatories (new staff)
- Analysis of training needs/updates in training
- Capturing/Celebration of positive messages relating to technology

Technology

Our Lady & St John uses a range of devices including PCs, laptops, Apple Macs. In order to safeguard pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use software that prevents unauthorised 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. In consultation with the Safeguarding Lead/DSL and the Headteacher, ICT Support Staff are responsible for ensuring that the filtering is appropriate. **(Appendix 5).**

Email Filtering – we use software that prevents any infected email being sent to or from 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 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 liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords All pupils and staff are encouraged to keep their passwords private. Passwords will be changed on a termly basis or in response to an incident where security has been compromised.

All pupils and staff should ensure that passwords are secure and complex. Passwords should have between 12-16 characters and be a mix of upper and lower case, numbers and special characters.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. ICT technical 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 pen 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 once the e-safety policy has been read and the Staff Acceptable Use Agreement signed and to pupils once the Pupil Acceptable Use Agreement has been signed by themselves and their parents/carers.

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. Pupils are permitted to use the school email system, and as such will be given their own email address.

Photos and videos – As part of the data collection process all parents are required to indicate if they consent to images/videos being taken.

Published content

Any information that is published whether in electronic or paper format must be professional in its presentation and content.

- Electronic communication should be treated as if it were being published on school headed paper and therefore written and presented in a professional manner.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- Content should be accurate and appropriate.
- Where pupils publish work, the content should be checked by a responsible adult.

Publishing Pupils' images and work

- Staff and pupils using any digital devices will ensure that they inform others before recording them and always use equipment in a respectful manner.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere, particularly in association with photographs.
- Written permission from parents or carers will be obtained as the pupil is admitted to Our Lady & St John, for photographs or video of pupils to be published.
- Where pupils' work is published, the school will ensure that the child's identity is protected.
- Where school events are being publicised, care will be taken not to reveal information that may put children or staff at risk e.g. the date and location of a trip.
- Staff should be aware of those pupils for whom permission from parent/carer has not been granted. Photographs of Looked After Children (LAC/Children in Our Care (CIOC) should not be taken/published without the consent of the Local Authority.

Parents using still or video cameras at school

In line with the Information Commissioner's Office, Our Lady & St John allows parents to record video and images during performances for personal use only.

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.

Social Networking

Our Lady & St John 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. Staff, parents and pupils are advised at all times to ensure that the content of their on-line activity remains appropriate and does not compromise their own or anyone else's safety.

Our Lady & St John has its own Twitter and Facebook account.

Some departments may choose to operate a Twitter account for their department. When doing so the account must be set up in such way that pupils can follow the department account but the department account does not follow the pupil.

The Safeguarding Lead/DSL will maintain a record of any department Twitter accounts.

Any posts on the school or department accounts should be considered carefully and must not bring Our Lady & St John Catholic College in to disrepute.

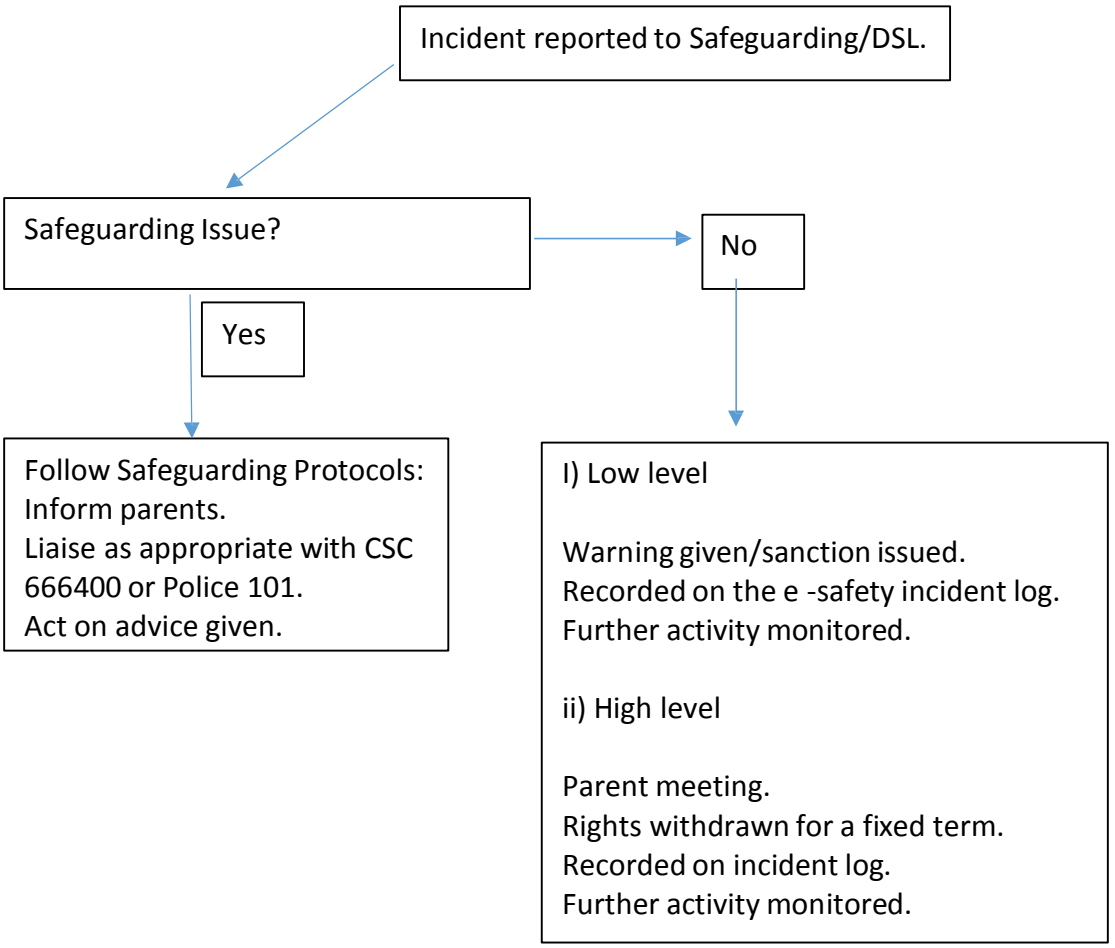
Our Lady & St John Catholic College cannot take any responsibility for views and opinions from third parties.

Removable media /mobile technology e.g. USB drives

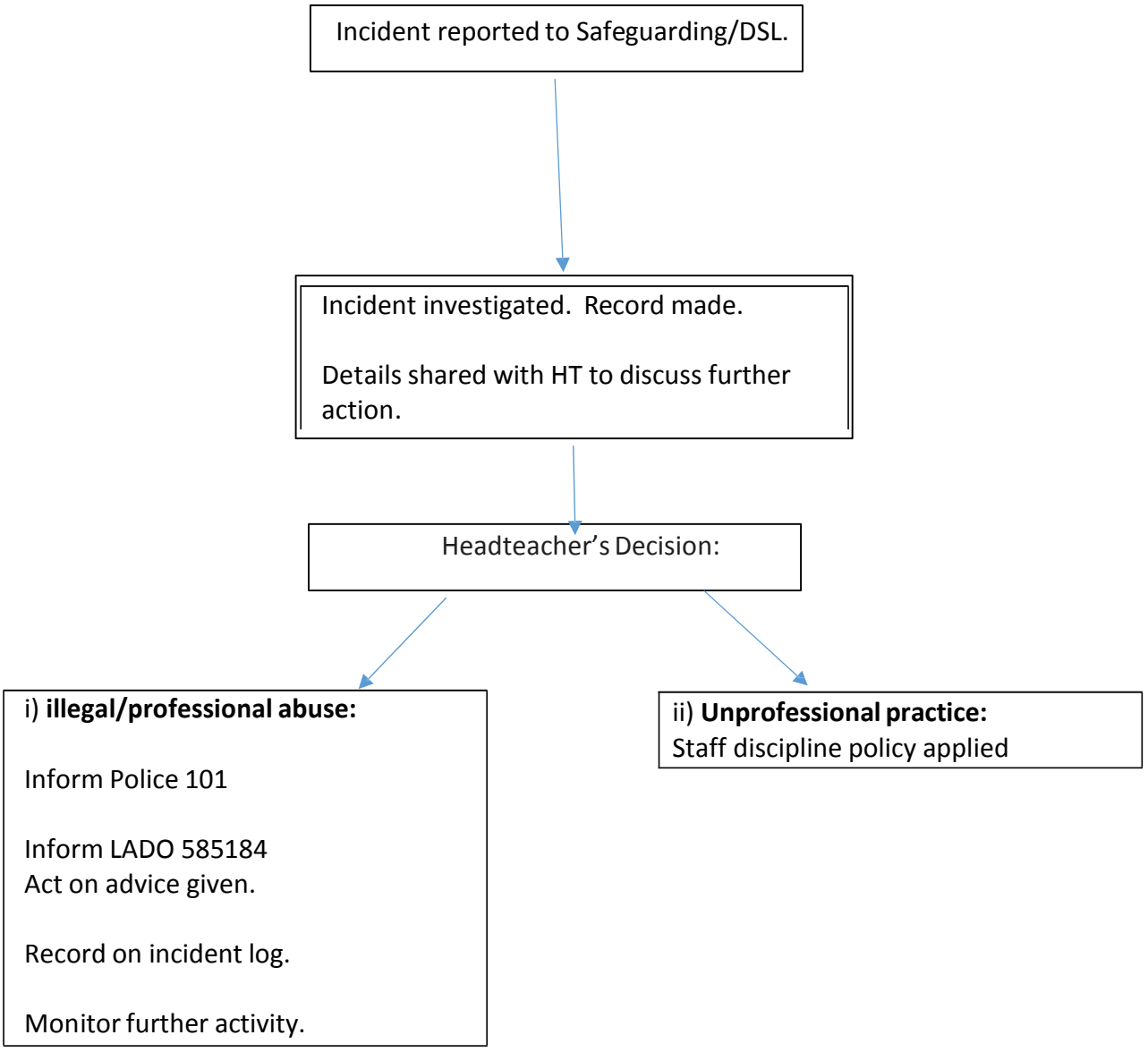
The school discourages the use of removable media. Staff are provided with alternative means of saving data.

Appendix 1

Responding to suspected or actual illegal/inappropriate misuse of ICT by pupils



Responding to suspected o r actual illegal/inappropriate misuse of ICT by staff



Appendix 2

Sexting

Definition

Whilst professionals refer to the issue as 'sexting' there is no clear definition of 'sexting'. Many professionals consider sexting to be 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the Internet.'

Legislation:

Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes a child taking an image of themselves if they are under 18.

The relevant legislation is contained in the Protection of Children Act 1978 (England and Wales) as amended in the Sexual Offences Act 2003 (England and Wales).

Handling disclosures/incidents

Staff will:

- Inform the DSL immediately and record on CPOMS.
- Record what the child says in the child's own words.
- Do not ask probing questions which may compromise any subsequent investigation.
- Under no circumstances should you request to see the image/text.

The DSL will then act in accordance with the agreed laid down procedures.

Appendix 3

Our Lady & St John Catholic College

Staff (and Volunteer) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and digital devices for educational and personal use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the internet and school digital devices.
- I understand that the rules set out in this agreement also apply to use of school digital devices out of school.
- ***I understand that the school discourages the use of removable media.***
- I understand that the school digital technology systems are intended for educational use only; the use of equipment should not be for personal gain.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- ***I will use complex passwords: 12-16 characters and be a mix of upper and lower case, numbers and special characters.***
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of to the Safeguarding Lead/DSL.

I will be professional in my communications and actions when using school devices:

- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use social networking for personal use that could undermine the school, its staff, parents or children.
- I will not become friends or followers with parents or pupils including former pupils under the age of 18, on personal social networks. No reference should be made on social media to pupils, parents /carers or school staff. (Personal opinions should not be attributed to the school or local authority. Security settings on personal social media profiles should be at their highest and regularly checked to minimise risk.)
- I will not engage in online discussion on personal matters relating to members of the school community.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- ***I will alert the ICT Network Manager of a termination to my employment so that permissions and access to the school systems can be removed.***

Staff are reminded that school data, including emails, is open to Subject Access Requests under the Data Protection Act and requests may be made under the Freedom of Information Act.

The school and the local authority have the responsibility to provide safe and secure access to digital devices and ensure the smooth running of the school:

- I will not use personal email addresses on the school ICT systems; – I will not use school email addresses for personal business. All email should be kept professional.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others or bring the school in to disrepute.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act).

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others in accordance with school policy; where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority in consultation with the Safeguarding Lead/DSL.
- I will immediately report to IT Services any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school digital devices and network (both in and out of school) and my own digital devices within these guidelines.

Staff Name: .....

Signed: .....

Date: .....

Appendix 4

E Safety – Pupil Acceptable Use Agreement

The school has installed computers with Internet access to help your learning. These rules will keep you safe and help us be fair to others:

- I will only access the system with my own login and password, which I will keep private;
- ***I will use complex passwords: 12-16 characters and be a mix of upper and lower case, numbers and special characters;***
- I will not access other people's accounts;
- I will only use the digital devices provided by school to complete my school work/homework;
- I understand that using the school's digital devices to access inappropriate materials such as 'adult', racist or offensive material is forbidden;
- I will only email people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.);
- I will not arrange to meet any stranger I have communicated with on-line;
- I will report any unpleasant material or messages sent to me. I understand that this report would be confidential and would help protect other people and myself;
- Internet use may be subject to monitoring. I understand that the school may check my school account and will monitor the Internet sites I visit;
- I understand that if I do not follow these rules then I may have my access withdrawn.

As a user of the digital devices (including emails and the Internet) provided by Our Lady & St John Catholic College, I agree to comply with the above rules for its use in a responsible way.

Pupil Name _____ Form _____

Pupil Signature _____ Date _____

Parent Agreement

As the parent or legal carer of the above named pupil I give permission for my son /daughter to use the digital devices (including emails and the Internet) provided by Our Lady & St John Catholic College.

I understand that whilst the school has taken measures to provide a safe learning environment, pupils remain accountable for their own actions.

I understand that some materials on the Internet may be objectionable (despite the filtering system) and

I accept responsibility for setting standards for my son/daughter to follow when using the Internet.

I understand that my son/daughter's Internet use will be monitored (whilst using their school account) and if inappropriate activity is identified appropriate action will be taken in line with the school's behaviour for learning policy. In the first instance access to the school network will be withdrawn.

I will encourage my son/daughter to use their own digital devices safely and support the school in adhering

to the school's policy on the restrictions around the use of personal digital devices in school.

I am aware there is an e-safety policy which can be found on the school's website.

Parent/Carer Name _____Date _____

Parent/Carer Signature _____Date _____

Appendix 5

Why we filter the Internet

Introduction

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.

Why do we Filter and Monitor?

Our Lady & St John will filter and Internet activity may be subject to monitoring.

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.
- 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.

We monitor for assurance:

- As much as possible that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

A right to privacy?

Everybody has a right to privacy, whether adult or child. However, in certain circumstances there is a reduced expectation of privacy. In the context of this policy, 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 is not used on the school network, but is used in school or for school business).