e-Safety Policy:

The Acceptable Use of the Internet and related Technologies

Contents

Our e-Safety Policy has been written using Becta guidance. It has been agreed by the Senior Leadership Team and approved by the governing body on 20.10.2016 and will be reviewed annually.

Next Review date: July 2017

SECTION 1: OVERVIEW

Context

The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom.

The Green Paper *Every Child Matters* and the provisions of the *Student Act 2004, Working Together to Safeguard Children,* sets out how organisations and individuals should work together to safeguard and promote the welfare of all students.

The ‘staying safe’ outcome includes aims that students and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation;
- safe from accidental injury and death;
- safe from bullying and discrimination;
- safe from crime and anti-social behaviour in and out of school;
- secure, stable and cared for.

Many of these aims apply equally to the ‘virtual world’ that students and young people will encounter whenever they use IT in its various forms. For example, we know that the internet has been used for grooming students and young people with the ultimate aim of exploiting them sexually; we know that IT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that students and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the ‘virtual’ or digital world as would be applied to the school’s physical buildings.

This Policy document is drawn up to protect all parties including the students and the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

Well embedded technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by students include:

- The Internet;
- e-mail;
- Instant messaging (often using simple web cams);
- Blogs (an on-line interactive diary);
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player);
- Social networking sites;
- Video broadcasting sites;
- Chat Rooms and forums;
- Gaming Sites;
- Music download sites;
- Mobile phones with camera and video functionality;
- Smart phones with e-mail, web functionality and cut down 'Office' applications;
- Learning Platform (the school uses Edmodo).

2. Whole school approach to the safe use of IT

Creating a safe IT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for students, staff and parents.

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Executive Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Executive Headteacher ensures that the policy is implemented and compliance with the policy is monitored. The responsibility for e-Safety has been designated to Mrs C Peaker, Acting Deputy Headteacher).

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a **'No Blame'** culture so students feel able to report any bullying, abuse or inappropriate materials.

We ensure this by adopting a firm belief and trust attitude to any reported incidents.

All staff should be familiar with the policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of student information/photographs and use of website;
- E-Bullying / Cyberbullying procedures;
- Their role in providing e-Safety education for students.

How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and students are given information about infringements of use and possible sanctions.

Our e-Safety Coordinator, Mrs C Peaker, Acting Deputy Headteacher acts as first point of contact for any complaint. Any reported complaint about staff misuse must be referred to the Executive Headteacher.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school / LA child protection procedures and must be reported to the School Safeguarding Officer (Mrs C Peaker).

SECTION 2: MANAGING THE INTERNET SAFELY

Managing the Internet Safely

This school:

- Maintains broadband connectivity through Virgin;
- Ensures any concerns about the system are communicated to the Network Manager, Mr P Evans) so that systems remain robust and protect students;
- Does not allow the sending or receiving of bulk data files (.zip)
- Ensures network health through appropriate anti-virus software etc and network set-up so staff and students cannot download executable files such as .exe / .com / .vbs etc;
- Ensures their network is ‘healthy’ by having the school IT technical team carry out regular audits;
- Ensures the Systems Administrator / network manager is up-to-date with regard to technology in education issues;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows students access to Internet logs;
- Uses individual log-ins for students and all other users;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Ensures students only publish within appropriately secure learning.

Policy procedures for teaching and learning:

This school:

- Supervises students' use, ***as far as is reasonable***, and is vigilant in learning resource areas where older students have more flexible access;
- We use an internal filtering system which blocks sites that fall into categories such as pornography, race hatred, extremism and radicalisation, gaming and sites of an illegal nature;
- Plans the curriculum content for Internet use to match students' ability;
- Is vigilant when conducting 'raw' image search with students e.g. Google is defaulted to safe search for images;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Network Manager (Mr P Evans). Our Network Manager reports to LDL when necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only uses approved system services for video conferencing activity;
- Only uses approved blogging or forums, such as on approved Learning Platform and blocks others;
- Only uses approved or checked webcam sites;
- Has blocked student access to music download or shopping;
- Requires students (and their parent/carer to individually sign an e-Safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Requires all staff to acknowledge that they had read this e-Safety document;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programmes;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures parents provide consent for students to use the Internet, as well as other IT technologies, as part of the e-Safety acceptable use agreement form at time of their daughter's / son's entry to the school;
- Makes information on reporting offensive materials, abuse / bullying etc. available for students, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – including the Police.

Education programme:

This school:

- Fosters a 'No Blame' environment that encourages students to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures students and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the Uniform Resource Locator (URL) to the teacher or Network Manager;
- Ensures students and staff know what to do if there is a cyber-bullying incident;
- Has a clear, progressive e-Safety education programme throughout all Key Stages, built on national guidance.
- Students are taught a range of skills and behaviours appropriate to their age and experience, such as:

  - to STOP and THINK before they CLICK;
  - to expect a wider range of content, both in level and in audience, than is found in the school resource centre or on TV;
  - to discriminate between fact, fiction and opinion;
  - to develop a range of strategies to validate and verify information before accepting its accuracy;
  - to skim and scan information;
  - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know some search engines / web sites that are more likely to bring effective results;
  - to know how to narrow down or refine a search;
  - to understand how search engines work;
  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - to understand 'Netiquette' behaviour when using an online environment such as a 'chat' / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
  - to not download any files – such as music files - without permission;
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
  - to have strategies for dealing with receipt of inappropriate materials.

- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Raises staff awareness of the e-Safety issues;
- Runs a rolling programme of advice, guidance and training for parents, including: suggestions for safe Internet use at home.

SECTION 3: MANAGING E-MAIL SAFELY

How will e-mail be managed?

E-mail is now an essential means of communication for staff in our school and increasingly for students and their families. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between students and staff, or for use in local and international school projects.

However, un-regulated e-mail can provide a means of access to a student that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Once e-mail is available it is difficult to control its content.

Procedures:

In the school context, **e-mail should not be considered private** and the school reserves the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of students and the preservation of human rights, both of which are covered by legislation.

The use of personal e-mail addresses, such as Hotmail, should be avoided by all working in schools and staff should use the school's systems wherever possible for professional purposes. **Personal information regarding staff and students, other than that held for registration, should not be sent by e-mail and must only be sent to specific staff and not general distribution lists. Any e mails staff send to all staff or other general distribution lists must first be approved by your line manager. Staff must seek permission from a member of the SLT before sending any e mails that are considered to be of a personal nature.**

Education:

Students need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of the school's e-Safety and anti-bullying education programme.

Students need to understand good 'netiquette' style of writing, and appropriate e-mail behaviour.

SECTION 4: GUIDELINES FOR USING DIGITAL IMAGES AND VIDEO SAFELY.

Developing a safe school web site:

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety.

Use of still and moving images:

Most importantly, care needs to be taken when using photographs or video footage of students on the school website. Consider using group photographs rather than photos of individual student. Do not use the first name and last name or give personal details such as home address of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

- **if the student is named, never use their photograph / video footage.**

- **if the photograph /video is used, never name the student.**

If showcasing examples of students work consider using only their first names or their form name, rather than their full names.

Only use images of students in suitable dress to reduce the risk of inappropriate use.

Photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, students should be advised why they are being taken.

Parental permission should be obtained before publishing any photographs, video footage etc of students on the school website or in a DVD. This ensures that parents are aware of the way the image of their child is representing the school. All parents are required to complete a Parental Permission Form but this should be checked as to whether permission has been granted before images are used.

Procedures:

Use excerpts of students' work such as from written work, scanned images of artwork, photographs of items designed and made in technology lessons or recorded performances for examination purposes. This allows students to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of students.

Links to any external websites should be thoroughly checked before inclusion on the school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by students should always be reviewed before publishing it on the school website. Make sure that the work does not include the full name of the student, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, check that students' work doesn't contain any statements that could be deemed defamatory or in any way damages the name and reputation of the school or undermines its' ethos.

The school ensures that it is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

If the website contains any guestbook, notice board or blog, they need to be monitored to ensure they do not contain personal details of staff or students.

If showcasing school -made digital video work, take care to ensure that students are not referred to by name on the video, and that students' full names are not given in credits at the end of the film.

Technical:

Digital images / video of students need to be stored securely on the school network and old images deleted after a reasonable period, or when the student has left the school.

In this school

- Uploading of information is restricted to administration officers with the necessary administration rights as decided by the school's e-Safety officer;
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of students are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use students' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of students in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students. Staff are also reminded to familiarise themselves with the Keeping Children Safe in Education 2016 Document;
- Students are taught to publish for a wide range of audiences which might include governors, parents or younger students as part of their IT scheme of work;
- Students are taught about how images can be abused in their e-Safety education programme.

SECTION 5: USING THE SCHOOL NETWORK, EQUIPMENT AND DATA SAFELY

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

- Ensures staff read and sign that they have understood the school's e-Safety policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides students with an individual network log-in username. The login details must not be saved on stand-alone computers around the school ;
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find them;
- Makes clear that students should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Students cannot run programs downloaded from the internet;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used to support their professional responsibilities and that they notify the school of any "significant personal use";
- Maintains equipment to ensure Health and Safety is followed;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Does not forward databases unless student names have been removed;
- Provides students and staff with access to content and resources through the approved Learning Platform (Edmodo) which staff and students access using their username and password;
- Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system;
- Follows LDL advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school IT systems regularly with regard to security;

SECTION 6: CYBER-BULLYING POLICY

The school Anti-Bullying Policy covers cyber bullying. It makes clear that use of the web, text messages, e-mail, video or audio to bully another student or member of staff will not be tolerated.

The policy makes explicit reference to cyber bullying and includes the following guidance for staff:

"Bullying can be done verbally, in writing or images, including through communication technology (cyber-bullying) e.g.: graffiti, text messaging, e-mail or postings on websites. It can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form.

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

- Advise the child not to respond to the message;
- Refer to relevant policies including e-Safety/acceptable use, anti-bullying and apply appropriate sanctions;
- Secure and preserve any evidence;
- Inform the school's e-Safety officer.

The e-Safety officer may decide to:

- Inform the sender's e-mail service provider;
- Notify parents of the student involved;
- Consider informing the police depending on the severity or repetitious nature of offence;
- Involve the school's Child Protection Officer.

If malicious or threatening comments are posted on an Internet site about a student or member of staff the school's Safeguarding Officer must be informed immediately. She will:

- Inform parents and request the comments be removed if the site is administered externally;
- Inform the Executive Headteacher;
- Secure and preserve any evidence;
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html;
- Endeavour to trace the origin and inform police as appropriate.

Students should be confident that a no-blame culture operates within the school when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

SECTION 7: INFRINGEMENTS AND POSSIBLE SANCTIONS

How will infringements be handled?

Students

Category A infringements

- Use of non-educational sites during lessons;
- Unauthorised use of email;
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends;
- Use of unauthorised instant messaging / social networking sites;
- Continued use of non-educational sites during lessons after being warned;
- Continued unauthorised use of email after being warned;
- Continued unauthorised use of mobile phone (or other new technologies) after being warned not to do so;
- Continued use of unauthorised instant messaging / chat rooms, social networking sites, News Groups.

Possible Sanctions: *School Behaviour Policy (applied as with any other classroom misbehaviour).*

Category B infringements

- Use of File-sharing software;
- Accidentally corrupting or destroying others' data without notifying a member of staff;
- Accidentally accessing offensive material and not logging off or notifying a member of staff.

Possible Sanctions: *Removal within classroom from IT equipment, Departmental detention, teacher / Head of department contacts home, teacher to inform e-Safety officer to invoke possible removal of Internet access rights for a period.*

Category C infringements

- Deliberately corrupting or destroying someone’s data, violating privacy of others;
- Sending an email or other electronic message that is regarded as harassment or of a bullying nature (one-off);
- Deliberately trying to access offensive or pornographic material;
- Any purchasing or ordering of items over the Internet;
- Transmission of commercial or advertising material.

Possible Sanctions: *Immediate removal from classroom, referral to Safeguarding Officers or a member of Senior Leadership with possible removal of Internet and/or Learning Platform access rights for a period, parents may be contacted.*

Category D infringements

- Continued sending of emails or other electronic messages regarded as harassment or of a bullying nature after being warned;

- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Possible Sanctions*: Referral to Safeguarding Officer or a member of SLT - involvement of relevant pastoral leader/ internal exclusion / exclusion / removal of equipment.*

Staff

Category A infringements (Misconduct)

- Use of the Internet for personal activities not related to professional development e.g. online shopping, personal e-mail, instant messaging etc. during times when they should be discharging their professional duties;
- Misuse of first level data security, e.g. wrongful use of passwords;
- Breaching copyright.

Possible Sanctions: *referral to Senior Line Manager (member of Leadership Team) / Executive Headteacher. Warning given.*

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school hardware or software;
- Installing unlicensed software on network;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute or compromising or undermining the ethos and religious charism of the school.
- Accessing any social networking sites using school equipment or personal devices whilst on school premises.
- Not having the highest possible security settings if using a social networking site or electronic form of communication outside of school and identifying yourself as an employee of Notre Dame. Making comments or displaying images that might be considered offensive to other colleagues or undermines or damages the ethos or reputation of the colleague or of the school.
- Communicating with any students past or present on social networking sites and will not store any images or information about students unless as part of specific school business and always on securely encrypted drives

Possible Sanctions*: Referral to Executive Headteacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police*

Other safeguarding actions:

- Immediately inform the e-Safety officer who will ask for the machine to be removed to a secure place to ensure that there is no further access to the device

- The school will instigate an audit of all IT equipment by an outside agency, such as the school's IT managed service providers - to ensure there is no risk of students accessing inappropriate materials in school,
- Safeguarding Officers will identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they may be instantly suspended. Normally there will be an investigation before disciplinary action is taken for any alleged offence. As part of the process the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's e-Safety / Acceptable Use Policy. All staff will be required to acknowledge that they have read the school's e-Safety Policy;
- Students will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours', students will sign an age appropriate e-Safety / acceptable use form;
- The school's e-Safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the Notre Dame;
- Information on reporting abuse / bullying etc will be made available for students, staff and parents;
- Staff are issued with the 'What to do if?' guide on e-Safety issues.

SECTION 8: ACCEPTABLE USE FORMS

IT Acceptable Use: Agreement Form [STAFF]
EMAIL / INTERNET / INTRANET / NETWORK USAGE POLICY

1. IT Acceptable Use: Agreement form [STAFF]

EMAIL / INTERNET / INTRANET / NETWORK USAGE POLICY

2. PARENTAL AGREEMENT FORM

Please refer to following page

IT Acceptable Use: Agreement form [STAFF]

- I will not use school equipment to access or store any resources or material that might in any way compromise or be considered inappropriate with regard to the ethos of our school.
- I will only use the approved, secure email system(s) for any college business.
- I will only send student or staff information to relevant/specific staff and not to general distribution lists.
- When sending information, particularly emails, to other colleagues, I will ensure that they do not contain highly personal or confidential information.
- I will ensure that any emails sent to all staff have first been approved by my Line Manager.
- I will obtain permission from a member of SLT prior to distributing any email that might be considered to be of a personal nature.
- I will not browse, download or send material that could be considered offensive, to colleagues or students, using college owned equipment or personal devices.
- I will report any repeated accidental access to inappropriate materials to the appropriate line manager.
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the college's network security and confidentiality protocols.
- I will not connect a computer or laptop to the network / Internet that does not have an up-to-date version of anti-virus software.
- I will not use personal digital cameras, camera phones, or any other device for taking or transferring images of students or colleagues without informing my line manager and then by seeking parental (on behalf of a student)/personal permission (in the case of an adult).
- I will ensure I am aware of digital safeguarding issues and the college's e-safety policy so they are appropriately embedded in my classroom practice and any other activity that involves students, past or present.
- I will not allow unauthorised individuals to access Email / Internet / Intranet.
- I understand that all Internet usage will be logged and this information could be made available to my Line Manager on request and misuse might result in disciplinary action.
- I agree and accept that any computer or laptop loaned to me by the college, is provided to support my professional responsibilities and must not be used to access, browse or store any inappropriate images or text that might compromise or undermine the ethos of the school.
- I will notify the college of any "significant personal use".
- I acknowledge that I have been strongly advised not to use social networking sites at all. If I do choose to use them outside of college, I will ensure that I have in place the highest available security settings. I will not identify myself or any of my colleagues as an employee of Notre Dame Catholic College and I will not make any comments or display any images that might in anyway be considered offensive to other colleagues or the ethos of the school. I will not access any social networking sites using college equipment or personal devices whilst on college premises.
- I will not communicate with any students past or present on social networking sites and will not store any images or information about students unless as part of specific college business and always on securely encrypted drives. I will ensure that any communication of mine will not bring the college into disrepute or tarnish the reputation of the college in any way.
- **I understand that failure to comply with the Usage Policy could lead to disciplinary action.**

I have read and agree to abide by the above Acceptable Usage Policy.

Signature____ Date _____________

Full Name: __________________________________ Job title ___________

Authorised Signature (Head Teacher) _______________________ **Date:** _________

Is this member of staff temporary? NO / YES If yes, contract end date: ____________
I approve this email account / connection to the Internet / Intranet.

Keeping safe: stop, think, before you click!

12 rules for responsible IT use.

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the college's computers for college work and homework.
2. I will only delete my own files.
3. I will not look at other people's files without their permission and I will not copy work from another student and claim it is my own.
4. I will keep my login and password secret.
5. I will not bring files into college without permission.
6. I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the college.
7. I will only e-mail people I know, or my teacher has approved.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
10. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends.
11. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
12. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

E-Safety Agreement Form

Parent / Carer name: ________________________________

Student name: ____

As the parent or legal guardian of the above student, I grant permission for my daughter or son to have access to use the Internet, e-mail and other IT facilities at college.

I know that my daughter or son has signed an e-Safety agreement form and that they have a copy of the 12 ‘Rules for Responsible IT Use’.

I accept that ultimately the college cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the college will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching e-Safety skills to students.

I understand that the college can check my child’s computer files, and the Internet sites they visit and that if they have concerns about their e-Safety or e-behaviour that they will contact me.

I will support the college by promoting safe use of the Internet and digital technology at home and will inform the college if I have any concerns over my child’s e-Safety.

Parent / Carer signature: _____________________________ **Date:** ___/___/___

Use of digital images - photography and video: I also agree to the college using photographs of my child or including them in video material. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the college, and for no other purpose.

Parent / Carer signature: _____________________________ **Date:** ___/___/___

Keeping safe: stop, think, before you click!

Student name: ____

I have read the college 'rules for responsible IT use'. My teacher has explained them to me.

□

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

□

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other IT in a safe and responsible way.

□

I understand that the college can check my computer files, and the Internet sites I visit and that if they have concerns about my safety, that they will contact my parent / carer.

□

Student's signature ____

Date: ___/___/___

SECTION 9: GUIDANCE: 'WHAT DO WE DO IF?'

An inappropriate website is accessed <u>unintentionally</u> in college by a student:

- Play the situation down; don't make it into a drama;
- Report to Pastoral Leader or e-Safety officer;
- Inform the college technicians and ensure the site is filtered.

An inappropriate website is accessed <u>intentionally</u> by a student:

- Inform Safeguarding Officer or a Member of SLT;
- Inform the e-Safety officer who will in turn inform college technicians and ensure the site is filtered out of the system.

An adult uses College IT equipment inappropriately:

- Ensure you have a colleague with you; do not view the misuse alone;
- Report the misuse immediately to the Executive Headteacher and ensure that there is no further access to the PC or laptop. The college / e-Safety officer will then consider the following course of action:
- If the material is offensive but not illegal, the college may decide to:
  - Remove the PC to a secure place;
  - Instigate an audit of all IT equipment by the colleges IT managed service providers to ensure there is no risk of students accessing inappropriate materials in the college;
  - Identify the precise details of the material;
  - Take appropriate disciplinary action;
  - Inform governors of the incident.
- In an extreme case where the material is of an illegal nature:
  - Remove the PC to a secure place and document what you have done;
  - Contact the local police and follow their advice.

Staff are asked to inform the E-Safety Officer if they unintentionally access a site that contains inappropriate materials.

A bullying incident directed at a student occurs through email or mobile phone technology, either inside or outside of college time:

- Advise the student not to respond to the message;
- Refer the matter to the school safeguarding officer

Malicious or threatening comments are posted on an Internet site about a student or member of staff:

- Inform the college safeguarding officer.

You are concerned that a student's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

- Report to and discuss with the named Safeguarding Officer in college **as soon as possible;**

Students should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.