NOTRE DAME SCHOOL E-SAFETY AND USE OF TECHNOLOGY POLICY

NOTRE DAME SCHOOL

Contents

1. Introduction and Scope

Safeguarding is a serious matter; at Notre Dame School (the School) we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as E-Safety is an area that is constantly evolving and as such this policy will be reviewed regularly or in response to an E-Safety incident. This Policy sits alongside other School policies, in particular:

- Safeguarding and Child Protection Policy
- Behaviour and Exclusions Policies
- Disciplinary and Grievance Policies
- Data Protection Policy
- Whistleblowing Policy
- Code of Conduct

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- contact: being subjected to harmful online interaction with other users; for example: child on child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If a member of staff feels their pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

2. Responsibilities

2.1 Governors

The Governing body will consider and ratify this E-Safety policy, and review it as required in light to changes to guidance and legislation. Governors are expected to follow the policy in the same way as volunteers are, including participating in E-Safety. Governors will receive reports on breaches of this policy and E-safety issues.

2.2 Head teachers

The Head teachers will ensure that:

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

2.3 E-Safety Officer

The day-to-day duty of E-Safety Officer is devolved to the ICT Manager. The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves 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 Head teacher.
- Advise the Head teacher and Governing body on all E-Safety matters.
- Engage with parents and the school community on E-Safety matters at school and/or at home.
- Liaise with other agencies as required.
- Retain responsibility for the E-Safety incident log; ensure staff know what to report and maintain the appropriate audit trail.

- Ensure any technical E-Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose.
- Make him/herself aware of any reporting function with technical E-Safety measures, i.e. internet filtering reporting function; liaise with the Head teachers and responsible governor to decide on what reports may be appropriate for viewing.
- Report to the Head teachers on recorded incidents and liaise with the Head teacher on any investigation and action in relation to e-incidents.

2.4 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 E-Safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user.
- Passwords are applied correctly to all users regardless of age.
- Being responsible for the IT infrastructure and that it is not open to misuse or malicious attack.
- Ensuring that users may only access the networks and devices through an enforced password protection policy.
- Keeping up to date with E-Safety technical information in order to carry out their role.

2.5 Designated Safeguarding Leads

Designated Safeguarding Leads have overall responsibility for online safety (more details contained in the Safeguarding and Child Protection Policy). They should be trained on E-Safety issues and aware of the implications that may arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate contact on-line with adults/strangers; and
- potential or actual incidents of grooming and cyber-bullying.

2.6 Staff

All Staff are to ensure that they:

- Understand the details of the policy. If anything is not understood it should be brought to the attention of the Head teachers or the E-Safety Officer.
- Any E-Safety incident is reported to the E-Safety Officer or in his/her absence to the Head teachers and an E-Safety Incident report is made (see Appendix 5).
- Fully understand the reporting flowcharts contained within this E-Safety policy (Appendix 4).
- Maintain awareness of school E-Safety policies and practices.
- Report any suspected misuse or problem to the Head Teacher or E-Safety Co-ordinator.
- Ensure that all digital communications with pupils / parents / carers/ fellow staff are on a professional level and conducted on school systems.
- Recognise relevant E-Safety in teaching activities and curriculum delivery.
- Ensure pupils understand and follow E-Safety policies, including the need to avoid plagiarism and uphold copyright regulations.
- Monitor the use of digital technologies (including mobile devices, cameras etc) during school activities.
- Ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

2.7 Pupils

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy (Appendix 2); any deviation or misuse of ICT equipment or services will be dealt with in accordance with the School's Behaviour Policy.

E-Safety is embedded into the School's curriculum; pupils 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.

Pupils are to ensure that they:

- are responsible for using school digital technology systems in accordance with the school acceptable use policy;
- will understand and follow E-Safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to understand policies on the use of mobile devices and digital cameras, the taking/using of images and cyber-bullying; and
- will understand that the E-Safety policy will include actions outside of school where related to school activities.

2.8 Parents and Carers

The School will provide opportunities for parents to gain skills and knowledge to help keep children safe online outside the school environment. Through parents' E-Safety lectures and school newsletters the school will keep parents up to date with new and emerging E-Safety risks, and will involve parents in strategies to ensure that students are empowered.

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 countersign the student Acceptable Use Policy (Appendix 2, 3 or 4) before any access can be granted to school ICT equipment or services.

Parents should follow school guidelines on:

- digital and video images taken at school events;
- access to parents' sections of the school website / pupil records; and
- their children's/pupils' personal devices in the school (where this is permitted).

The School will adopt a **zero tolerance approach** to any cyber bullying issues, that all staff will challenge any abusive behaviour between pupils that comes to their notice and will report to the DSL immediately any issues of this nature. Please see the School's Safeguarding and Child Protection Policy for further details on child-on-child abuse.

2.9 Community Users / Contractors

Where such groups have access to school networks/devices, they will be expected to provide signed acceptance to abide by school E-Safety policies and procedures.

3. Technology

Notre Dame School uses a range of devices including PC's, laptops, Apple Macs. To safeguard the students and in order to prevent loss of personal data we employ the following assistive technology:

- **Internet Filtering** – we use Securly software 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 E-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head teacher.
- **Monitoring & Filtering -** we use Filter, a cloud-based web filter designed exclusively for schools, this helps keep students safe with features designed to allow visibility into online activity, download or email reports, and block inappropriate sites instantly. Filter are partnered with Securly Aware which allows for early intervention.

- **Email Filtering** – we use Libra ESVA Email Filter software that prevents any infected email 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. Links in emails are sandboxed to prevent access to infected websites.
- **Data Security** –no data is to leave the school on a non-password protected device. Any breach (i.e. loss/theft of device such as laptop) is to be brought to the attention of the Head teacher or E-Safety Officer immediately. Further information regarding the security of data is in the Data Protection Policy.
- **Passwords** – all staff and students will be unable to access any device (except for the Prep School iPads) without a unique username and password.
- **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 Head teacher if there are any concerns. All USB peripherals such as USB memory sticks are to be scanned for viruses before use.
- **USB memory sticks** - Students are prohibited from using USB sticks at School. Staff may use encrypted USB sticks.

4. Safe Use

4.1 Internet

The use of the Internet in school is a privilege, not a right. Internet use will be granted to staff upon signing the relevant Acceptable Use Policy.

4.2 Email

All staff are reminded that emails are subject to Freedom of Information and Subject Access 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.

Students are permitted to use the school email system and as such will be given their own email address. The email address will be made up of their first initial and surname, e.g. jsmith@notredame.co.uk

4.3 Social Networking

There are many social networking services available. The School is fully supportive of social networking as a tool to engage with parents and the wider school community. The following social media services are permitted for use within Notre Dame School and have been appropriately risk assessed and are managed by the E-Safety Officer:

- Twitter
- Facebook
- LinkedIn
- Flickr
- Instagram

Should staff wish to use other social media, permission must first be sought via the E-Safety Officer. Any new service will be risk assessed before use is permitted.

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

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be set to “moderated”.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a licence 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 E-Safety incident is to be brought to the immediate attention of the E-Safety Officer, or in his/her absence the Head teachers. The E-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, Notre Dame School will have an annual programme of training which is suitable to the audience.
- E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.
- E-Safety is covered within the ICT curriculum for Years 1 to 9. Lessons cover various age-appropriate issues. The Head of ICT in each school plans the content for these lessons.
- As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.
- E-Safety advice can be found on Firefly.

4.4 Pupils' mobile phones

Access to cellular networks is not permitted by pupils in school and any instances will be dealt with via the Behaviour policy. Pupils below Year 10 are not allowed a mobile device during the school day. Prep pupils who travel by coach are allowed to bring their mobile devices to School but must leave them with the Front Office during the school day.

4.5 Visitors

There are visitor logons available for visitors to the school to be able to use a school computer. This has no access to any school data. Visitors can also separate Wi-Fi for the purpose of accessing the Internet from their own devices. In both cases their access to the Internet is filtered in the usual way.

5. Monitoring and Filtering

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

The school subscribe to multiple systems that monitor school devices and the school network.

5.1 Internet Filter

The Internet Filter monitors and blocks access to, what the School deems inappropriate websites or content. It also keeps a log of all activity which is reviewed by the IT team and where necessary, the DSLs.

5.2 Safeguarding

Our safeguarding software monitors all inappropriate behaviour on all school systems. The School sets behavioural threshold on the system. When these thresholds are met, the system will automatically email the DSLs. All inappropriate behaviour is logged and can be viewed by DSLs.

The School's monitoring systems will be able to monitor online behaviour such as, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).

5.3 Classroom Monitoring

Our classroom monitoring software allows the class teacher to monitor what each pupil is accessing or viewing on their School issued one to one device during a lesson. It will allow the teacher to freeze screens during class, control other screens, and share their own screen with their class. This software is not available for devices brought from home.

6. Retention of digital data

Any information from email folders that is necessary for the school to keep for longer, including personal information (e.g. for a reason set out in the school privacy notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

7. Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, contact the Data Controller or Head teacher immediately.

The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

8. Staff use of mobile phones

The aim of this policy is to promote safe and appropriate practice through establishing clear and robust guidelines for staff. The School's intention is to provide an environment in which pupils and staff are safe from images being recorded and inappropriately used, in turn eliminating the following concerns:

- Staff being distracted from their work with pupils.
- The inappropriate use of mobile phones and cameras around children.

Staff must adhere to the following:

- Staff use of mobile phones during the working day must be discreet and appropriate and not in the presence of pupils.
- Mobile phones should be switched off and out of view during lesson times.

- The use of mobile phones during teaching time is strictly forbidden.
- Mobile phone calls may only be taken during staff breaks and not in the presence of pupils.
- Staff must not take images of pupils or store data relating to pupils on their mobile phones.
- Staff and volunteers are not permitted to use their personal phones for contacting pupils and their families within or outside the setting unless authorised by SLT in advance.
- Staff should not access content that is not suitable for professional use during working hours whilst on the school site.
- On school trips staff may use their own phones but only for personal use (preferably out of sight of pupils) or to contact school or other staff, not to contact pupils or parents or to take any photographs or video footage of any students. Staff using their phones on coaches or public transport for personal use is acceptable.
- Photos related to school activities must not be posted on social media from personal accounts.

Appendix 1

Acceptable Use of IT - STAFF

This Policy applies to the use of:

- all internet and electronic mail facilities, multi-user computers, workstations, micro-computers, and any networks connecting them provided by the School;
- all hardware owned, leased, rented or otherwise provided by a member of staff and connected to or otherwise accessing School networks or other facilities;

Staff may use their own devices in school and can connect to the staff WIFI. If for any reason they need to connect to the internal network they would need to speak to the IT Manager. The contents of the School's IT resources and communications systems are the School's property. The storage of personal files on School IT resources is prohibited. Such data is deemed to belong to the School.

The system must be used only in connection with your duties for which the School employs you.

Limited use of E-mail and Internet facilities for personal purposes is permitted. The School acknowledges that personal use may occur from time to time. Any such use must be in accordance with this Policy and must not disrupt staff duties. Abuse or excessive use of the e-mail and/or Internet will be dealt with through the disciplinary procedure.

You must not interfere with the work of others or the system itself. The facilities must be used in a responsible manner - in particular, you must not:

- create, transmit or cause to be transmitted material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence, and you must not create, transmit or cause to be transmitted offensive obscene or indecent material;
- create, transmit or cause to be transmitted defamatory material;
- create, transmit or cause to be transmitted material such that the copyright of another person is infringed;
- download any files unless virus scanned;
- use networked computing equipment for playing computer games;
- gain deliberate unauthorised access to facilities or services accessible via local or national networks;
- transmit by e-mail any confidential information of the School otherwise than in the normal course of your duties;
- send any message internally or externally which is abusive, humiliating, hostile, intimidating or angry;
- you must not gain unauthorised access to or violate the privacy of other people's files, corrupt or destroy other people's data or disrupt the work of other people;
- disclose passwords to third parties without the consent of the School;
- you must not email messages to "All Staff" unless you have the permission of a member of the Senior Leadership/Management Team;
- when using Facebook, Twitter and similar social media sites, please do so with caution and thought. Remember your audience, if you have linked up with pupils and parents and because of public access to the information, the utmost discretion should be used when posting information and pictures; and
- use your school email address for personal use such as online purchases.

You must:

- always observe this policy and note the disciplinary consequences of non-compliance which in the case of a gross breach or repeated breach of the Policy, may lead to dismissal;
- ensure that you use the School standard e-mail sign off and disclaimer for all external e-mail;
- produce and write e-mails with the care normally given to any form of written communication; and
- appreciate that electronic mail is relatively insecure and consider security needs and confidentiality before transmission.

The School reserves the right to monitor staff communications in order to establish the existence of facts, ascertain compliance with regulatory or self-regulatory procedures, monitor standards which are achieved by persons using the system in the course of their duties and for staff training purposes, to prevent or detect crime, to investigate or detect unauthorised use of the School's telecommunication system, to ensure the effective operation of the system such as protecting against viruses, backing up and making routine interceptions such as forwarding e-mails to correct destinations and to gain access to routine business communications for instance checking voice mail and e-mail when staff are on holiday or on sick leave.

All Heads of Departments have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and if necessary enforcing this policy by taking action when behaviour falls below its requirements.

Relationship with other School policies
When communicating online, staff are expected to adhere to all School policies and be aware their conduct does not alter because they are online. For example, staff are prohibited from using social media to:

- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations they may have relating to confidentiality;
- breach our Disciplinary Rules;
- defame or disparage the School or our affiliates, parents, staff, pupils, business partners, suppliers, vendors or other stakeholders;
- harass or bully other staff in any way or breach our Anti-harassment and bullying policy;
- unlawfully discriminate against other staff or third parties or breach our Equal Opportunities policy;
- breach our Data Protection policy (for example, never disclose personal information about a colleague, pupil or parent online);
- breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

Staff must also be aware of the risks to internet security that social media presents and so must take any extra measures necessary not to allow any of their actions on social media sites to create vulnerability to any School systems.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Communications with the Media
You must not speak to or communicate with the media on matters concerning the School's affairs or regarding your position in the School without the prior written permission.

Responsible use of social media
This policy applies to the use of social media for both business and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff or any other IT equipment. Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details so far as this is consistent with the right of an individual to private and family life.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Staff must be aware that their role comes with responsibilities and they must adhere to the School's strict approach to social media.

Staff must:

- ensure that wherever possible their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives;
- obtain the prior written approval of the Head teacher, to the wording of any personal profile which you intend to create where the School is named or mentioned on a social networking site;
- seek approval from the Head teacher before they speak about or make any comments on behalf of the School on the internet or through any social networking site;
- report to their Head of Department or Line Manager immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School;
- immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other School policy;
- consider whether a particular posting puts their effectiveness as a teacher at risk;
- post only what they want the world to see.

Staff must not:

- provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the school and create legal liability for both the author of the reference and the school;
- post or publish on the internet or on any social networking site, any reference to the School, your colleagues, parents or pupils;
- use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations;
- discuss pupils or colleagues or publicly criticise the School or staff;
- post images that include pupils;
- initiate friendships with pupils on any personal social network sites;
- accept pupils as friends on any such sites; staff must decline any pupil- initiated friend requests (unless from former pupils, as per the Safeguarding Policy);
- use social networking sites as part of the educational process e.g. as a way of reminding pupils about essay titles and deadlines.

Personal use of social media

We recognise that staff may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal or political solicitations or promotion of outside organisations unrelated to the organisation's business are also prohibited. Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our IT systems. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.
We prohibit staff from using their work email address for any personal use of social media.

Staff should have no expectation of privacy in any message, file, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

Please confirm that you understand and accept this policy by signing below and returning the signed copy to HR.

Name of Staff Member

Signed	
Date	

Appendix 2

Acceptable Use of IT – SENIOR PUPILS

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational 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.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating on-line.
- 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).
- If I arrange to meet people off-line that I have communicated with on-line (which I understand is not recommended by the school), I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will act as I expect others to act toward me.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices in school if I have permission.
- If I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, 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 install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, withdrawal from activities, contact with parents, exclusion from school, and in the event of illegal activities, involvement of the police.

BYOD devices

I acknowledge that:

- Bringing on premises or infecting the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information is in violation of Acceptable Use Policy Agreement.
- Notre Dame School has the right to collect and examine any device that is suspected of causing problems or was the source of an attack or virus infection.
- Notre Dame School has the right to inspect files on any device bought into school and as part of a school activity, irrespective of if it has been the cause of a problem/attack/virus (This covers devices that may contain objectionable material obtained offsite and stored on my device).
- It is my responsibility for the repair of any malfunctioning/damaged devices. The ICT support Department can provide assistance with configuring devices onto the wireless network but does not supply technical services for student owned devices.
- Personal devices are fully charged prior to bringing it to school and runs off its own battery while at school.
- Responsibility to keep the device secure rests with me. Notre Dame School, nor its staff or employees, is not liable for any device stolen or damaged at school. If a device is stolen or damaged, it will be handled through the school similar to other personal effects. It is recommended that your device is marked in some way to physically identify your device from others. Additionally, protective cases for technology are encouraged.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed)
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, intranet, website etc.

Name of Pupil	
Class	
Signed	
Date	
Parent Countersignature	

Appendix 3 - Pupil Acceptable Use Agreement – for Year 5-6

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational 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.

Notre Dame will try to ensure that all pupils will have good access to digital technologies to enhance their learning and will, in return, expect the girls to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating on-line.
- 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 immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices in school if I have permission. I understand that, if I do use my own devices in the *school* I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:
- I should 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 try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, withdrawal from activities, contact with parents, exclusion from school, and in the event of illegal activities, involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:
- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed)
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, intranet, website etc.

Name of Pupil	
Class	
Signed	

Date	
Parent Countersignature	

Appendix 4 – Pupil Acceptable Use Agreement – for Year 1-4

Pupil Acceptable Use Policy Agreement– for younger pupils (Y1-4)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

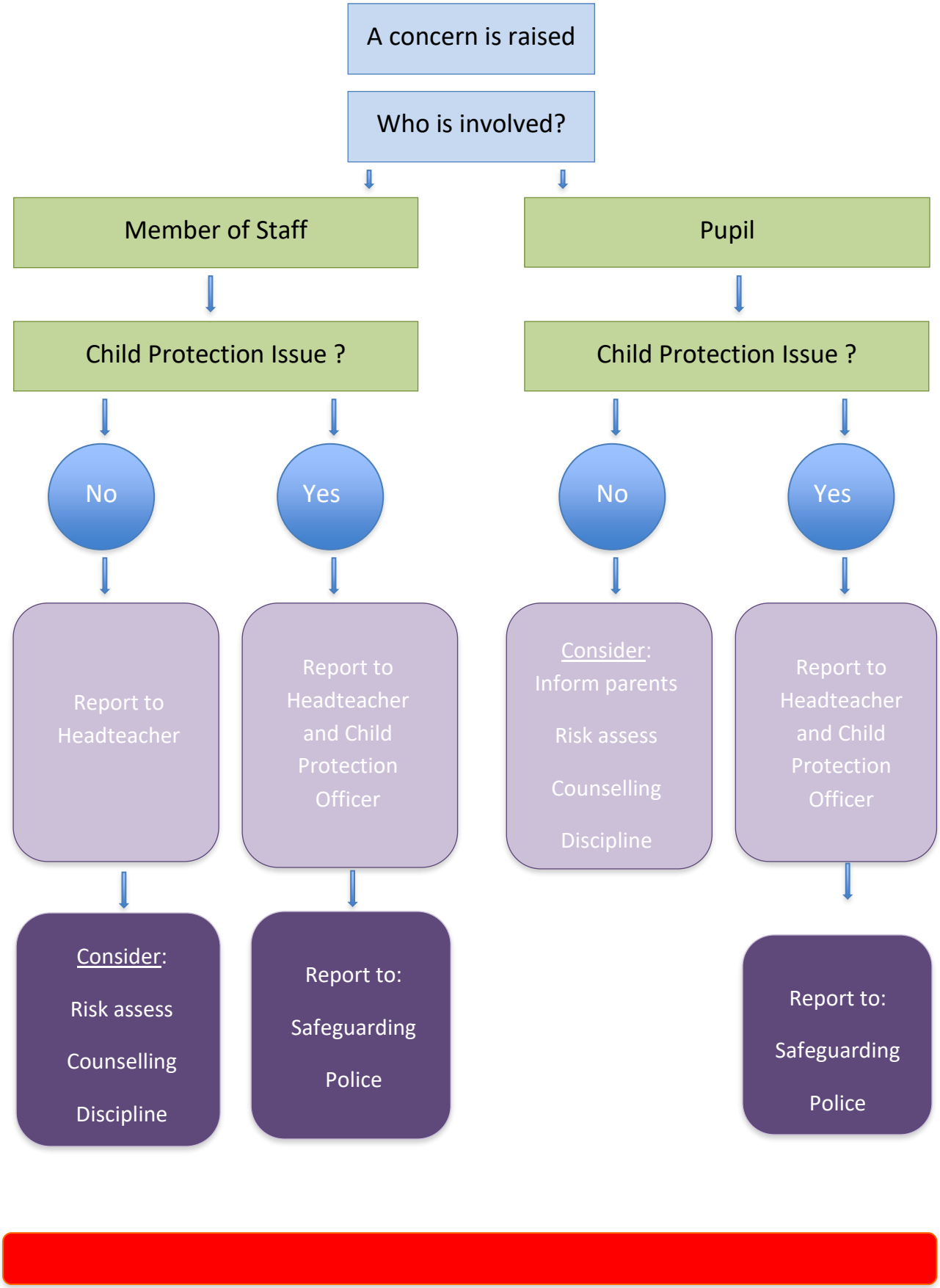
Signed (child):……

Signed (parent): ……..

Appendix 5 E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, E-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Appendix 6 - Inappropriate and Illegal Activity Flowcharts



Illegal Activity Flowchart