ONLINE SAFETY POLICY (INCLUDING ACCEPTABLE USE POLICIES)

This Online Safety policy was approved by the Governing Body on:	September 2021
The implementation of this Online Safety policy will be monitored by the:	Headteacher, Senior Leadership Team and the Online Safety Leader
Monitoring will take place at regular intervals:	September each year.
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	An Online Safety report will be generated once per term and shared at Full Governor's Meetings.
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2022
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LEA Safeguarding Officer, Police

Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

St. Ignatius Catholic Primary School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, St. Ignatius Catholic Primary School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Our Online Policy, as part of the wider Safeguarding and Child Protection agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings.

Our Vision

St. Ignatius Catholic Primary Schools vision for Online Safety is to provide a diverse, balanced and relevant approach to the use of technology. Our pupils will be encouraged to maximise the benefits and opportunities that technology has to offer by following the guidelines in the Lancashire Primary Online Safety framework. We will ensure that children will learn in a safe and secure environment so that they can learn effectively. Our aim is that pupils will be equipped with the skills and knowledge to use 21st Century technology appropriately and responsibly. Pupils will be taught how to recognise the risks associated with this technology and how to deal with them, both inside and outside the school environment.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

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

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- commerce : risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

Our Golden Rules for Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

We don't give out personal information on any online forums.

Vision for E-Safety

We provide a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer.

We ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.
Children are equipped with the skills and knowledge to use technology appropriately and responsibly.

We teach how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.
All users in our school community understand why there is a need for an E-Safety Policy.

Roles and Responsibilities

Governing Body

The governing body is accountable for ensuring that out school has effective policies and procedures in place: as such they will:
Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing these incidents.

Lyndon Jones (Chair) who has overall responsibility for the governance of online safety at the school who will:

Keep up to date with the emerging risks and threats through technology use

Receive regular updates from the head teacher in regards to training, identified risks and any incidents.

Meet with the Online Safety Lead Deputy Headteacher Miss S. Kellett

Report to governors on online safety issues that arise.

Head teacher and Senior Leaders

Reporting to the governing body, the head teacher has overall responsibility for online safety within our school. The day to day management of this will be delegated to a member of staff, the online safety lead, as indicated below.
The Head teacher will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, e.g. students, all staff, SLT and governing body, parents.
- The designated online safety lead has had appropriate CPD in order to undertake the day to day duties.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- All online safety incidents are dealt with promptly and appropriately. The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents later in this policy)
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online safety Co-ordinator / Officer.

Online safety Lead

The day to day duty of online safety officer is devolved to: Sarah Kellett
The online safety officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/ herself with the latest research and available resources for school and home use
- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing this policy regularly along with other related document and bring any matters to the attention of the Head teacher.
- Advise the Head teacher, governing body on all online safety matters.
- Meets with the online safety governor regularly meets regularly to discuss current issues, review incident logs and filtering / change control logs
- Provides training and advice for staff and ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Retain responsibility for the online safety incident log, ensure staff know what to report and ensure the appropriate audit trail as well as a log of incidents to inform future online safety developments. Engage with parents and the school community on online safety matters at school and/or home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Ensure any technical online safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the LA and ICT technical support.
- Make him/ herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function, liaise with the Head teacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

- Technical support staff are responsible for ensuring that:
- The IT technical infrastructure is secure; this will include at a minimum:
- Anti-virus is fit for purpose, up to date and applied to all capable devices.
- Windows (or other operating systems) updates are regularly monitored and devices updated as appropriate.
- Any online safety technical solutions such as internet filtering are operating correctly.

- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and the Head teacher.
- Passwords may not be applied to shared pupil areas. Passwords for staff will be a minimum of 8 characters.
- The IT system administrator password is to be changed on a bi-monthly basis.
- Machines are encrypted and memory sticks containing pupil information are encrypted.
- The school meets required online safety technical requirements and any Local Authority / other relevant body Online safety Policy / Guidance that may apply.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet/ email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and/ or Online safety Lead for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school / academy policies

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the head teacher or online safety officer.
- They have an up to date awareness of online safety matters and the current school policy and practices.
- They have read, understood, signed and abide by the acceptable use policy **SEE APPENDIX B**
- All digital communication with pupils and parents/ carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities and implement current policies with regard to the use of digital technologies, mobile devices, cameras etc in lessons.
- Pupils understand and follow the online safety and acceptable use policies and have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- In lessons where internet use is pre-planned students / pupils should be 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
- Any online safety incident is to be reported to the online safety lead, and/ or the head teacher and recorded in an online safety incident log.
- The reporting flowcharts contained within this online safety policy are to be understood.

Senior Designated Person for Safeguarding:

Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Security and data management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment.

The *Lancashire ICT Security Framework* (published 2005) should be consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school. In line with the requirements of the General Data Protection Regulation (GDPR, 2018) and the Data Protection Act (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.
- Staff are aware that they should only use approved means to access, store and dispose of confidential data.

- We do not use cloud storage facilities e.g. Dropbox / OneDrive or external storage related to software used for creation of children's profiles (especially in Early Years).
- Key computers are password protected.
- No devices containing data allowed to be removed from the school premises.
- Staff are not allowed to store data on personal devices.

Photographs/Videos of Children - Consent

We have *written* consent from parents for photographs and/or videos of their children to be taken or used. Parents are consulted regarding material for: newsletter, website and local media.

Verbal consent is not considered acceptable.

A record of non-consent is maintained by the bursar and disseminated to all teaching staff.

Students are not allowed to take photos to include in portfolios maintained by trainees/ students not directly employed by the setting.

Taking Photographs / Video

Photographs/videos are only taken using school owned equipment. The use of personal equipment to store images should be avoided.

Storage of Photographs / Video

Storage of such visual images must be stored on password protected computers in school and not in the 'cloud'.

CCTV, Video Conferencing, Zoom and Webcams

During lockdown 2020/21, when the school was only partially open, Zoom video conferencingwas used to maintain contact with pupils not in school.

Parents agreed to adhere to a set of terms and conditions for use of Zoom with their children,which included: online etiquette, appropriate backgrounds and content.

Managing the network and technical support

ICT service centre Lancashire Services (Tom- Technical support officer) is responsible for managing the security of the school network and for installing all programmes.
This is reviewed annually.

Dealing with incidents

Incident Log

The school has established an incident log to record and monitor incidents/offences. This is stored in the school Office and is audited on a regular basis by the e-Safety Champion or a designated member of the Senior Leadership Team.

Illegal Offences

Any suspected illegal material or activity will be brought to the immediate attention of the Headteacher & referred to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF) who will take responsibility for all aspects of investigation. The school recognises the importance of following correct procedures & will not conduct investigations independently. If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (Appendix 1) for responding to online safety incidents and report immediately to the Headteacher and the police.

Inappropriate Usage

Accidental access to inappropriate materials occurs very rarely & children & adults are aware of the necessary actions to take (minimise webpage, turn monitor off & tell a trusted adult immediately). The adult will then inform Sarah Kellett and log the incident in the Online Safety incident log found in the office. These procedures are regularly reinforced as an integral part of ICT sessions. Details will be entered in the Incident Log and reported to LGfL Lightspeed if necessary. Never personally investigate, interfere with or share evidence as you

may inadvertently be committing an illegal offence.
It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Education and training

Children are taught that third-party contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies. As such, they could be at risk from:

- Peer-on-peer abuse
- Grooming
- Cyberbullying in all forms
- Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords.

Conduct

Children are made aware that their personal online behaviour can increase the likelihood of,or cause harm to themselves and others, for example,

- Privacy issues, including disclosure of personal information, digital footprint and onlinereputation.
- Health and well-being - amount of time spent online (internet or gaming).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII(self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership – such asmusic and film).

E-Safety - across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' e-Safety.
Our school provides relevant, flexible and engaging e-Safety education to all children as part of their curriculum entitlement. This includes: regular, planned e-Safety teaching within a range of curriculum areas.

Filtering and virus protection

The school subscribes to the Lancashire Grid for Learning/BT Lancashire Services broadband & high level internet content filtering is provided by default. Sophos Anti-Virus software is included in the school's subscription & this is configured to receive regular updates. On rare occasions, unsuitable content may get past the filter & pupils are taught to follow set procedures if this occurs (report instantly to staff & turn off monitor).

Raising Awareness

'Parents/Carers often either underestimate or do not realise how often children come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.' (Byron Report, 2008)
School will offer regular opportunities for parents/carers to be informed about Online Safety. These will include the benefits and risks of using various technologies. School will do this by:

- School newsletters, homework books, school website,
- Holding an Online Safety Awareness session at least annually based on demand
- Promote external Online Safety resources/online materials as a handout to all children at National eSafety Week & thereafter.

Online Safety – Raising Governors' awareness

Governors with specific responsibilities for Online Safety, ICT, Child Protection and Safeguarding Children & Anti- Bullying will be required to keep themselves up to date. This may be through discussion at Governor meetings, attendance at Local Authority or staff/parent/carer meetings. Our Online Safety Governor is Lyndon Jones.

Standards and Inspection

Greater emphasis must be placed on monitoring child protection and safeguarding procedures within our school as technology is moving forward at such a rapid pace. School will consider the following to encompass this by ensuring:

- Online Safety incidents are monitored, recorded and reviewed
- New technologies are risk assessed & that they are included in the Online Safety Policy where appropriate
- Online Safety Champion to make necessary any changes to this policy, following regular reported Online Safety incidents which may affect practise within school
- Online Safety Champion to make staff, parents/carers, pupils and governors informed of any changes to policy and practice throughout the school year by use of class ICT lessons, school newsletter/website, staff/governor meetings.

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review bothphysical and network security regularly and monitor who has access to the system consulting withthe LA where appropriate.

- Pupils use is monitored
- Staff use is monitored by the Head
- All staff are issued with their own username and password for network access. Students use class log-ins, which have restricted access to our server.

  NB. External hard drives and pen sticks are not to be used on our PCs and laptops

- A 'guest' log-in is available for use of our internet facility for supply staff/ visitors

- Pupils are issued with a class username and password and understand that this must not be shared

Communication technologies

Email

In our school the following statements reflect our practice in the use of email.

- All staff have access to the Lancashire Grid for Learning service as the preferred school e-mail system & this is used for any work related activity
- Only official email addresses are used to contact staff
- Only key named staff are permitted to manage confidential information
- E-Mail communication is routinely monitored in accordance with Acceptable Use Policy
- Incidents of SPAM are reported to the ICT Coordinator, Sarah Kellett
- Threatening or offensive e-mails are reported to the Online Safety Champion & evidence collected
- Pupils do not have individual e-mail accounts. If required as part of curriculum work, teachers create class accounts (within specific closed environment software packages) & manage these for the duration of a project, after which they are closed.

- In the event of a class requiring an email account for curriculum work, Sarah Kellett will create an account to be used solely for the purpose of the educational activity e.g. Skype. The username and

password will not be shared with the pupils.

In our school the following statements outline what we consider to be acceptable and unacceptable use of the following:

Mobile telephones

- *See separate Mobile Phone and Camera Policy*

Instant Messaging

- Pupils to have restricted access to Zoom as a part of carefully planned school activities (&with Head teacher permission). Zoom will only be used, under direct control of the teacher,as a class learning tool.

Web sites and other online publications

- The school website is managed & monitored by a key named member of staff.
- Content uploaded to the website is carefully controlled to ensure high levels of security &adherence to AUP requirements.
- All staff are aware of the importance of ensuring online safety when submitting items forpublication on the school website.
- Pupils' work is not displayed in other digital locations

Video conferencing

- Zoom is the preferred video conferencing tool as it is easily accessible & straight forward to set up.
- Video conferencing will only take place as part of carefully planned & approved education projects (with Headteacher permission).
- Parental written consent will be secured before video conferencing is undertaken.
- Teachers will be directly responsible for managing video conferencing sessions.
- Under no circumstances will children undertake video conferencing independently.
- Video conference partners will be carefully & systematically vetted to ensure pupil safety(e.g. use of trusted sources – schools, museums, education departments).
- Written & signed agreements will be in place prior to video conferencing sessions in order to ensure preservation of copyright, privacy and Intellectual Property Rights (IPR).
- Full training for staff will be provided prior to commencing video conferencing activities.
- Video conferencing will be managed by a teaching team, not individual staff.

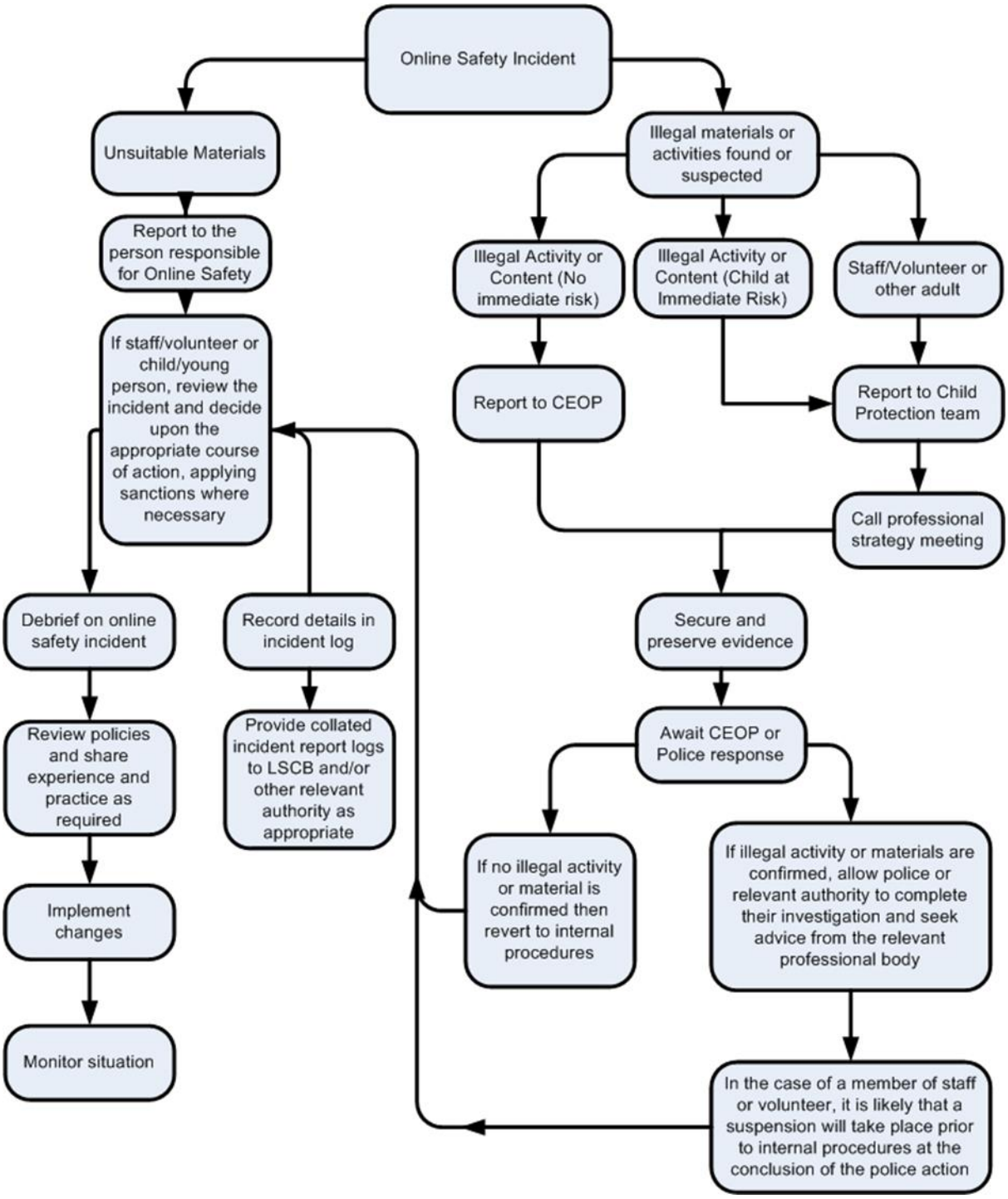
Acceptable Use Policy (AUP)

The school actively promotes responsible, safe & courteous behaviour when accessing & using technology. Issues such as internet safety, copyright, plagiarism, cyberbullying & respect for others' work are addressed regularly as a part of ongoing class projects. Staff act as positive role models & trusted adults & have signed AUP agreements. The school has adapted the Lancashire AUP template agreement format for future AUP policy development, modification & use (see appendix)

Policy updated September 2021

Policy review date: September 2022

Appendix 1


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

APPENDIX 1

Example of Image Consent Letter/Form to Parents

St. Ignatius Square
Preston
PR1 1TT
Telephone 01772 555252
Fax 01772 254834
Website: www.saint-ignatius.com
Head Teacher: Mr C.J. Hough

Dear Parents,

In line with new data protection rules taking effect in the UK from 25th May, 2018 (GDPR), we would like you to confirm your choices regarding photos and videos of your child.

These, as well as copies of children's work, are invaluable to showcase and celebrate the activities undertaken by pupils in school and we would, therefore, appreciate you taking the time to confirm your consent.

** Please note that should this form not be returned your child will not be photographed or videoed.**

Please tick (✓) the relevant box(es) below and return this form to school.

Name of child…… DOB……

I consent for photos and videos of my child, as well as copies of their work, to be used on the school website and in the school newsletter. ☐

I consent for photos of my child to be used in their own books (exercise books, EYFS Learning Journals, Evidence me). ☐

I consent for photos of my child to be used in other children's books (exercise books, EYFS Learning Journals, Evidence me), e.g. group shots.

I consent for photos of my child to be shared with local media e.g. newspaper or marketing. ☐

I do NOT give consent for the school to use any of the above. ☐

If you change your mind at any time, please let us know by contacting the school office.

Parent or carer's signature: …… Date: ……..

Please note that your signature confirms your agreement to treat any photos and videos containing images of other children as for your own personal use (whether taken by school or by parents, e.g. at school shows). This means that information cannot be shared or published in any way, e.g. photos cannot be published on social media or displayed in a public place.

Please note that the Privacy Notice is available on the school website: https://saint-ignatius.com/

APPENDIX 2

Example of ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will be an active participant in e-Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of *Sarah Kellett*
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's e-Safety policy and help children to be safe and responsible

APPENDIX 3

in their use of ICT and related technologies.

I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature .....

Date .....

Full Name (PRINT)

Position/Role .....

APPENDIX 3

Example of ICT Acceptable Use Policy (AUP) –
Students, Supply Teachers, Visitors, Guests etc.
To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature
I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date ……

Full Name **……** (PRINT)

Position/Role ……

APPENDIX 4
ICT Acceptable Use Policy – Children

These rules reflect the content of our school's e-Safety Policy. It is important that parents/carers read and discuss the following statements with their children, understanding and agreeing to follow the school rules regarding the use of ICT, including the use of the Internet.

- I will only use ICT in school for school purposes.
- I will not bring equipment, e.g. a mobile phone or mobile games console, into school unless specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class email address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access, inappropriate websites.
- If I accidentally find anything inappropriate, I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open or delete my own files.
- I will not attempt to download or install anything on the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my e-Safety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy (this may be viewed on the school's website: https://saint-ignatius.com/

We have discussed this Acceptable Use Policy and **.....** [print child's name] agrees to follow the e-Safety rules and to support the safe use of ICT at Dt. Ignatius R.C. Primary School.

Parent/Carer Name **.....** (print)

Parent/Carer Signature……

Class …….

Date ……

This A.U.P. must be signed and returned before any access to school systems is allowed.

APPENDIX 5

ICT Acceptable Use Policy (AUP) – Example Letter to Parents

Dear Parent/Carer,

The use of ICT, including the Internet, e-mail, learning platforms and mobile technologies, are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network sites that incorporate age-restriction policies, where the minimum acceptable age is at least 13 years. Any child who is below the acceptable age and who sets up or uses such a site is in clear breach of the site's privacy policy and/or terms and conditions. We, therefore, actively discourage suchpractices in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School E-Safety Policy, and alongside the school's Behaviour and Safeguarding Policies, outlines those principles we expect our children to uphold for both their own benefit and that of the wider school community.

Your support in achieving these aims is essential and I would, therefore, ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Our school provider operates a filtering system that restricts access to inappropriate materials. Whilst every effort is made to ensure that suitable restrictions are in place, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the school's Internet facilities.

If you would like to find out more about e-Safety for parents and carers, please visit the Lancashire e-Safety website:

http://www.lancsngfl.ac.uk/esafety

If you have any concerns or would like to discuss the use of ICT in school, please contact Cathy Callus.

Yours sincerely,

Chris Hough

APPENDIX 6

Example of E-Safety Incident Log

Date/Time	Incident Name of pupils/staff involved	Action taken

APPENDIX 7

Zoom Parental Agreement

Dear Parents,

Please read the following agreement, which sets out guidelines for use of Zoom with children learning at home.

Parent/Pupil Video Conferencing Agreement

We ask that:

- You access Zoom through parent / guardian accounts and make sure that the name of user is the child's first name only. This is so the hosting teacher can identify who is in the waiting room and will be able to let them into the session. Any names the teacher cannot identify, or have not signed the agreement below, will not be allowed to join the session.

- You, or an appropriate adult, are present in the room during the call and appropriate behaviour and language must be maintained at all times.

- Children are in a suitable environment during the call and that they are appropriately dressed.

- Household members are aware that the call is taking place and background noises and conversations can be picked up.

- You do not share the meeting login details with anyone outside of your household.

- You do not record the session or post or share sound, images or video clips of the teacher or other children that attend the Zoom session.

*****If there is a breach of the above rules, the child will be removed from the session and put into the waiting room or the call will be ended for all users.**

We will:

- Use the waiting room feature on Zoom, which will be administered by the hosting teacher.

- Use secure passwords to keep sessions secure.

- Mute children at times to allow others to speak and to improve sound clarity.

- Not use the live recording facility but may take screen shots to share on social media where we have permission to do so.

Please note: Unlike when we are in school, your child will be using your internet connection, which may not have the controls and firewall settings that we have when we are at school. We encourage you to review your home internet settings.

In participating or allowing your child to participate in online/remote learning, you are acknowledging that you understand that your child's image and voice will be transmitted via the Internet, into the homes of other pupils and staff. You are also acknowledging that the school, while taking measures to ensure secure transmission, cannot guarantee complete confidentiality (see pupil rules above) of your child's image/voice while participating in online learning.

Parents must also understand and agree that recording and/or dissemination of a child's or a staff member's voice and/or image is a serious school rule violation that may subject a child to the loss of online privileges and/or other disciplinary action, as appropriate. This may, in extreme cases result in a report to the appropriate authorities and the potential issuance of criminal charges. The parent and pupil agree that by participating in these online activities, they or any individual present in the pupil's household will not, without express written authorisation from school personnel, audio/video record or transmit other student or staff voices, images, or work product.

Please e-sign this document and return it to bursar@st-ignatius.lancs.sch.uk to agree to the terms setout above.

I agree to the terms of use for Zoom video calls for my child ……

E-signed: _____ (Please type name) Date:_____