Our Lady Immaculate Catholic Primary School Online Safety Policy

Introduction.

This Policy is designed to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely and is addressed as part of the wider duty of care to which all who work in schools are bound.

We are required as a school, through their Online Safety Policy, to ensure that we meet our statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

As a school we are subject to an increased level of scrutiny of our online safety practices by Ofsted Inspectors during inspections. From 2015 we have additional duties under the Counter Terrorism and Securities Act 2015 which requires us a school to ensure that children are safe from terrorist and extremist material on the internet.

Due to the ever changing nature of digital technologies, it is best practice that the school reviews the Online Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Development/Monitoring/Review of this Policy

This Online Safety policy has been developed by a working group made up of Louise Roberts and Chris Bowcock. Responsible for reviewing the policy is a group made up of any of the following people or groups:

- Headteacher/Deputy Headteacher/Senior Leaders
- Computing Curriculum Co-ordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Community users

Consultation with the whole school community has taken place through a range of formal and informal meetings and children and adult questionnaires.

Schedule for Development/Monitoring/Review

This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	
The implementation of this Online Safety policy will be monitored by the Head Teacher	*Mrs Catherine Sergeant.*
Monitoring will take place at regular intervals:	*See computing curriculum monitoring schedule. Attached appendix*
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:	*Annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new	*September 2017*

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:	
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Child Line, Police, CEOP*

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor namely Claire Powell. The role of the Online Safety Governor will be

- to hold regular meetings with the Online Safety Co-ordinator attendance at Online Safety Group meetings

- regular monitoring of online safety incident logs

- regular monitoring of filtering/change control logs

- reporting to relevant Governors meeting

Headteacher and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator 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 –The Headteacher are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator:

- leads the Online Safety Group

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

- provides training and advice for staff

- liaises with the Local Authority / relevant body

- liaises with school technical staff

- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,

- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs

- reports regularly to Senior Leadership Team

Network Manager/Technical staff:

It is also important that the managed service provider is fully aware of the school Online Safety Policy and procedures.

The Network Manager for ICT / Computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack

- that the school meets required online safety technical requirements and any Local Authority other relevant body Online Safety Policy/Guidance that may apply.

- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- 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/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader; Online Safety Coordinator for investigation/action and or sanction

- that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:
- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher/Senior Leader /Online Safety Coordinator for investigation/action/sanction
- all digital communications with students/pupils/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
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- 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

Designated Safeguarding Lead

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

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Coordinator (or other relevant person, as above) with:
- the production/review/monitoring of the school Online Safety Policy/documents.
- the production/review/monitoring of the school filtering policy and requests for filtering changes.

- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/and information about national or local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education –Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is

therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- To respect everyone's privacy and in some cases protection, parents/ carers are not allowed to take photos or images of the children. The school will publish all photos or images in a controlled and safe place.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary

- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.
The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data transfer/storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

This is an area of rapidly developing technologies and uses. As a school we will need to discuss and agree how we intend to implement and use these technologies eg we do not allow pupils to use mobile phones in lessons. This section may also be influenced by the age of the pupils.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	owed with staff permission	Not allowed
Mobile phones may be brought to the school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones / cameras								
Use of other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school/, or on school network								
Use of school email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

When using communication technologies, the school considers the following as good practice:
- Users must immediately report, to the nominated person – in accordance with the school, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*