The purpose of this policy is to:

- set out the key principles expected of all members of the school community at St Vincent de Paul Catholic Primary School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of St Vincent de Paul Catholic Primary School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

Scope (from SWGfL)
This policy applies to all members of St Vincent de Paul’s school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St Vincent de Paul Catholic Primary School.

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 e-safety behaviour that take place out of school.

<table>
<thead>
<tr>
<th>Role</th>
<th>Key Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headteacher/ Designated Child Protection Lead</td>
<td>To take overall responsibility for e-safety provision</td>
</tr>
<tr>
<td></td>
<td>To take overall responsibility for data and data security (SIRO)</td>
</tr>
<tr>
<td></td>
<td>To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL</td>
</tr>
<tr>
<td></td>
<td>To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant</td>
</tr>
<tr>
<td></td>
<td>To be aware of procedures to be followed in the event of a serious e-safety incident.</td>
</tr>
<tr>
<td></td>
<td>To receive regular monitoring reports from the E-Safety Co-ordinator.</td>
</tr>
<tr>
<td></td>
<td>To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)</td>
</tr>
<tr>
<td>Role</td>
<td>Key Responsibilities</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **E-Safety Coordinator**    | • takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents  
• promotes an awareness and commitment to e-safeguarding throughout the school community  
• ensures that e-safety education is embedded across the curriculum  
• liaises with school ICT technical staff  
• To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs  
• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident  
• To ensure that an e-safety incident log is kept up to date  
• facilitates training and advice for all staff  
• liaises with the Local Authority and relevant agencies  
• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection 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 and use of social media                                                                                                                                                                                                                                           |
| **Governors / E-safety governor** | • To ensure that the school follows all current e-safety advice to keep the children and staff safe  
• To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor  
• To support the school in encouraging parents and the wider community to become engaged in e-safety activities  
• The role of the E-Safety Governor will include:  
  • regular review with the E-Safety Co-ordinator / Officer ( including e-safety incident logs, filtering / change control logs )                                                                                                                                               |
| **Computing Curriculum Leader** | • To oversee the delivery of the e-safety element of the Computing curriculum  
• To liaise with the e-safety coordinator regularly                                                                                                                                                                                                                                                                                   |
| **Network Manager/technician** | • To report any e-safety related issues that arises, to the e-safety coordinator.  
• To ensure that users may only access the school’s networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed  
• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)  
• To ensure the security of the school ICT system  
• To ensure that access controls / encryption exist to protect                                                                                                                                                                                                                      |
<table>
<thead>
<tr>
<th>Role</th>
<th>Key Responsibilities</th>
</tr>
</thead>
</table>
| Role                              | personal and sensitive information held on school-owned devices  
• the school’s policy on web filtering is applied and updated on a regular basis  
• LGfL is informed of issues relating to the filtering applied by the Grid  
• that he / she keeps up to date with the school’s e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant  
• that the use of the network / Learning Platform/remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Headteacher for investigation / action / sanction  
• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.  
• To keep up-to-date documentation of the school’s e-security and technical procedures |
| LEARNING PLATFORM                  | Leader  
• To ensure that all data held on pupils on the LEARNING PLATFORM is adequately protected                                                                                                                                                                                                                                                          |
| Data Manager                       | • To ensure that all data held on pupils on the school office machines have appropriate access controls in place                                                                                                                                                                                                                                      |
| LGfL Nominated                     | contact(s)  
• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts                                                                                                                                                                                                                      |
| Teachers                           | • To embed e-safety issues in all aspects of the curriculum and other school activities  
• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)  
• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws                                                                                                                                 |
| All staff                          | • To read, understand and help promote the school’s e-safety policies and guidance  
• To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy  
• To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices  
• To report any suspected misuse or problem to the e-safety coordinator  
• To maintain an awareness of current e-safety issues and guidance e.g. through CPD  
• To model safe, responsible and professional behaviours in their own use of technology  
• To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. |
<table>
<thead>
<tr>
<th>Role</th>
<th>Key Responsibilities</th>
</tr>
</thead>
</table>
| **Pupils**      | • Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils)  
                   • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations  
                   • to understand the importance of reporting abuse, misuse or access to inappropriate materials  
                   • to know what action to take if they or someone they know feels worried or vulnerable when using online technology.  
                   • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices.  
                   • To know and understand school policy on the taking / use of images and on cyber-bullying.  
                   • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school  
                   • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home  
                   • to help the school in the creation/ review of e-safety policies  |
| **Parents/carers** | • to support the school in promoting e-safety and endorse the Parents’ Acceptable Use Agreement which includes the pupils’ use of the Internet and the school’s use of photographic and video images  
                   • to read, understand and promote the school Pupil Acceptable Use Agreement with their children  
                   • to access the school website in accordance with the relevant school Acceptable Use Agreement.  
                   • to consult with the school if they have any concerns about their children’s use of technology  |
| **External groups** | • Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school |
Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/LEARNING PLATFORM/staffroom/classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

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

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by classteacher/E-Safety Coordinator/Headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - referral to LA/Police.

- Our Headteacher acts as first points of contact for any complaint.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school