OUR LADY & ST PHILOMENA'S CATHOLIC PRIMARY SCHOOL

ACCEPTABLE USE OF ICT POLICY – SAFEGUARDING

SEPTEMBER 2025

POLICY STATEMENT

This policy aims:

- To safeguard children and young people at Our Lady & St Philomena's Catholic Primary School by promoting appropriate and acceptable use of information and communication technology.
- To outline the roles and responsibilities of all individuals at Our Lady & St Philomena's Catholic Primary School who have access to and / are users of work-related ICT systems.
- To ensure all ICT users at Our Lady & St Philomena's Catholic Primary School have an awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

SCOPE

This policy will apply to all individuals at Our Lady & St Philomena's Catholic Primary School who have access to and/ or users of work-related ICT systems. This will include children and young people, parents / carers, staff members, volunteers and students, Governors, visitors and contractors. This list is not exhaustive.

Parents / carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that takes place on-site, and, where relevant, off site.

ROLES and RESPONSIBILITIES

The Headteacher has overall responsibility for ensuring that online safety is an integral part of everyday safeguarding practice. This will include ensuring that:

- Staff receive appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are applied to the use / non-use of personal ICT equipment by all individuals who come into contact with Our Lady & St Philomena's
- Catholic Primary School. This includes the personal use of work-related resources.
- This policy is implemented, monitored and reviewed annually, and all updates are shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are open and transparent.

- Allegations of misuse or known incidents will be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies where applicable.
- Effective online safeguarding support systems are put in place e.g. filtering controls, secure networks and virus protection.
- Access to the Designated Safeguarding Lead (DSL) is available at all times, or in their absence to the Deputy Safeguarding Lead.

The DSL will be responsible for ensuring:

- Agreed policies and procedures are implemented in practice.
- All updates, issues and concerns are communicated to all ICT users.
- The importance of online safety in relation to safeguarding is understood by all ICT users.
- The training, learning and development requirements of staff are monitored and additional training needs identified and provided for.
- An appropriate level of authorisation is given to ICT users. Not all levels of authorisation will be the same – this will depend on the position, role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities where deemed appropriate.
- Any concerns and incidents must be reported in a timely manner in line with the agreed procedures.
- The learning and development plans address online safety.
- A safe ICT learning environment is promoted and maintained.

Staff members will ensure:

- Reporting any concerns in relation to alleged misuse or known incidents as soon as possible, in line with agreed procedures.
- ICT equipment is checked before use and all relevant security systems judged to be operational.
- Awareness is raised of any new or potential issues, and any risks which could be encountered as a result.
- Children and young people are supported and protected in their use of online technologies – enabling them to use safe ICT in a safe and responsible manner.
- Online safety information is presented to children and young people appropriate to their age and stage of development.
- Children and young people know how to recognise and report a concern.
- All relevant policies and procedures are adhered to at all times.
- Appropriate training is undertaken.

Children and young people are encouraged to:

- Be active, independent and responsible learners who follow the school's policy and procedures.
- Abide by the Acceptable Use Agreement.

- Report any concerns to an adult.

Parents / carers are made aware of the Acceptable Use Policy and Procedures to share responsibility for their actions and behaviours.

- A copy of the Acceptable Use Policy is provided to parents / carers.
- It is expected that parents / carers will explain and discuss this policy with their child to ensure that it is understood and agreed.
- Children will be encouraged to sign the Acceptable Use Agreement alongside their parent / carer where appropriate. Records of all signed agreements will be kept on file.
- Parents / carers will not be allowed to use personal technologies (e.g. mobile phones) on school's premises.

ACCEPTABLE USE BY STAFF, GOVERNORS and VOLUNTEERS

Staff, Governors and volunteers are enabled to use work based online technologies:

- To access age-appropriate resources for children and young people
- For research and information purposes
- For study support

All staff, Governors and volunteers will be subject to authorised use as agreed by the Designated Safeguarding Lead (DSL).

All staff, Governors and volunteers will be provided with a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they must sign, date and return. This will be kept on file.

Authorised users will have their own individual password to access a filtered internet service provider. Users are generally not permitted to disclose their password to others unless required to do so by law or where requested to do so by the Designated Safeguarding Lead. All computers and related equipment that can process personal data should be locked when unattended to prevent unauthorised access.

In the event of misuse by staff, Governors or volunteers

In the event of an allegation of misuse by a staff member, Governor or volunteer, a report should be made to the school's Designated Safeguarding Lead or the Chair of Governors immediately. Should the allegation be made against the Designated Safeguarding Lead, a report should be made to the Deputy DSL and the Headteacher.

Procedures must be followed as appropriate in line with the ICT Misuse Procedure, Safeguarding Policy and / or Disciplinary Procedures.

Should allegations relate to abuse or unlawful activity, Liverpool Children's Services, the Local Authority Designated Officer (LADO), Ofsted and / or the Police will be informed as applicable.

Acceptable use by children and young people

The Acceptable Use Policy and Agreement are used to inform children and young people of behaviours which are appropriate and others which are deemed unacceptable. This will allow children and young people to take some degree of responsibility for their own actions, understanding the risks and likely sanctions.

In the event of misuse by children and young people

Should a child or young person misuse ICT, the following sanctions will be applied:

- STEP 1: In the event of deliberate misuse, the parents / carer will be informed of the issue. The child or young person may be temporarily suspended from the particular activity.
- STEP 2: Further incidents of misuse could lead to the child or young person being suspended from using the internet or relevant technology for an increased period of time. The parent / carer will be invited to discuss the incident in more detail with Headteacher and the most appropriate action will be agreed.
- STEP 3: The sanctions for misuse can be escalated at any stage, if considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. If a child or young person is considered to be at risk of significant harm, the Safeguarding Policy will be applied. Allegations of serious misuse will be reported to the most appropriate agency e.g. Children's Services.

In the event that a child or young person accidentally accesses inappropriate material, it must be reported to an adult immediately. Appropriate action must be taken to hide or minimise the window. The computer must NOT be switched off, nor the page closed, until investigations have taken place and reported to the Local Authority.

Acceptable use by visitors, contractors and others

All guidelines in respect of Acceptable Use of Technologies must be adhered to by any visitors or contractors.