ST JOSEPH'S CATHOLIC PRIMARY SCHOOL

COMPUTING & DIGITAL SAFEGUARDING POLICY

Reviewed: September 2025

To be reviewed: September 2027

ST JOSEPH'S CATHOLIC PRIMARY SCHOOL
COMPUTING POLICY

COMPUTING AT ST JOSEPH'S

This Computing Policy outlines our comprehensive approach to teaching Computing at St Joseph's, in accordance with the 2014 National Curriculum in England, and in line with Ofsted expectations. Our commitment is to ensure that all learners develop a strong understanding of computing concepts, foster a positive attitude towards digital learning, and achieve their full potential in Computing. Through a carefully planned and engaging curriculum, we aim to equip pupils with the knowledge and skills needed to thrive in a digital world, while promoting safe, responsible, and creative use of technology.

VISION STATEMENT

At St Joseph's, our vision is to provide a high-quality computing education that prepares children for life in a digital age. We aim to develop confident, digitally literate learners who can use technology safely, creatively, and effectively. Through a broad and balanced curriculum, pupils will gain experience in computer science, information technology, and digital literacy, enabling them to understand how technology works, how to use it purposefully, and how to stay safe online.

INTENT

At St Joseph's, our intent is to deliver a computing curriculum that enables pupils to understand the principles of computer science, including logic, algorithms, and data representation. We aim to develop children's ability to use technology to create, communicate, and solve problems. Pupils will learn to use a range of digital tools and software confidently and responsibly. Online safety is embedded throughout the curriculum to ensure children understand how to protect themselves and others in a digital environment. We are committed to ensuring that computing is accessible to all learners and that it supports the development of skills needed for future learning and employment.

IMPLEMENTATION

At our school, Computing is taught as a discrete subject across all year groups, following a two-year rolling programme to accommodate our mixed-age classes. The curriculum is structured to ensure progression in knowledge and skills across the three strands: computer science, information technology, and digital literacy. Lessons are practical and engaging, using a variety of devices, platforms, and software to support learning. Teachers use resources such as Oak Academy, Barefoot Computing, and Purple Mash to enhance delivery and ensure alignment with the National Curriculum. Assessment is ongoing and informs planning,

ensuring that all pupils are supported and challenged appropriately. Enrichment opportunities, including themed days, coding clubs, and cross-curricular projects, further enhance pupils' experiences and engagement with computing.

IMPACT

The impact of our Computing curriculum is that pupils leave St Joseph's with a secure understanding of key computing concepts and the ability to apply their digital skills confidently and responsibly. They are able to use technology to create content, solve problems, and communicate effectively. Pupils demonstrate an awareness of online safety and understand how to behave responsibly in digital environments. Assessment outcomes, pupil voice, and work scrutiny show that children make good progress and enjoy their computing learning. Our aim is for every child to leave primary school digitally literate and well prepared for the technological demands of secondary education and beyond.

ASSESSMENT

Assessment in Computing is used to monitor pupils' understanding, track progress, and inform future teaching. Both formative and summative assessment strategies are used throughout the year. Formative assessment takes place through questioning, observation, and review of digital work, allowing teachers to identify misconceptions and adapt teaching accordingly. Summative assessments, such as end-of-unit tasks, digital projects, and quizzes, provide a more formal measure of pupils' attainment. These assessments evaluate children's ability to apply computing vocabulary, use software tools effectively, and demonstrate understanding of key concepts. Attainment and progress are recorded in our in-house tracking system to support planning and transition.

RETRIEVAL

At St Joseph's, retrieval practice is used in Computing to help pupils consolidate and retain key knowledge over time. Teachers regularly provide opportunities for children to revisit prior learning, both within units and across year groups. Before starting a new topic, pupils reflect on previously taught concepts, helping them make connections and build on their understanding. Lessons often begin with short quizzes, recap activities, or discussions that prompt pupils to recall computing terminology, coding principles, or online safety rules. These activities strengthen memory and improve long-term retention by encouraging pupils to retrieve information independently. This approach supports deeper learning and helps pupils become more confident in applying their computing knowledge in a range of contexts.

PLANNING

At St Joseph's, Computing is planned as a discrete subject and is supported by high-quality resources including Purple Mash and Oak Academy. These resources align with the National Curriculum and enhance teaching by providing accessible, engaging content. Due to our mixed-age classes, we follow a two-year rolling programme to ensure full coverage of the Computing curriculum. Planning is carefully sequenced to ensure progression and continuity across year groups, allowing children to build on prior knowledge and develop their digital skills over time. In addition to regular lessons, we incorporate themed days and whole-school activities, such as Safer Internet Day and coding challenges, which provide opportunities for enrichment and practical exploration.

CONTINUOUS IMPROVEMENT

At St Joseph's, we are committed to the continuous improvement of Computing teaching and learning. Regular reviews of teaching practices and curriculum implementation are conducted to maintain high standards and ensure effective delivery. Feedback is gathered from staff, pupils, and parents to identify strengths and areas for development. Pupil performance data is analysed to inform strategic decisions about curriculum planning, teaching approaches, and resource allocation. These findings are shared with the Senior Management Team and discussed with staff to guide improvements. Outcomes are reported to the Governors through the Curriculum Committee, ensuring accountability and a shared commitment to excellence in Computing education.

ROLES AND RESPONSIBILITIES

The following section outlines the e-safety roles and responsibilities of individuals and groups within St Joseph's.

The Governing Body

Governors are responsible for the approval of the Digital Safeguarding Policy and for reviewing its effectiveness. This is carried out by the Curriculum and Pupils Committee, which receives regular updates on e-safety incidents and monitoring reports. Mr Mike Wormald is our nominated Digital Safeguarding Governor; he also serves as the Safeguarding and Child Protection Governor.

The role of the E-Safety Governor includes:

- Holding annual meetings with the Digital Safeguarding Leader (Mr Adam Malley)
- Conducting annual monitoring of the Digital Safeguarding incident logs
- Reviewing the filtering and change control logs annually
- Reporting annually to the Full Governing Body

HEADTEACHER AND SENIOR LEADERS

The Headteacher has a duty of care to ensure the safety of all members of the school community, including digital safeguarding. While the overall responsibility lies with the Headteacher, the day-to-day management of e-safety is delegated to all members of the teaching staff. The Headteacher and at least one other member of the Senior Leadership Team are familiar with the procedures to follow in the event of a serious digital safeguarding allegation involving a member of staff.

It is the Headteacher's responsibility to ensure that relevant staff receive appropriate training to carry out their digital safeguarding roles effectively and to support the training of other colleagues where necessary. A system is in place to monitor and support staff who undertake internal e-safety monitoring roles, providing both a safety net and professional support.

HEADTEACHER / DESIGNATED SENIOR LEAD / BACK-UP SENIOR LEAD

At St Joseph's Catholic Primary School Wrightington, the Headteacher, Miss Gleeson, also serves as the Designated Senior Lead for Safeguarding and holds day-to-day responsibility for Digital Safeguarding. Her role includes leading the development and regular review of the school's Digital Safeguarding policies and documentation. She ensures that all staff are aware of the procedures to follow in the event of a Digital Safeguarding incident and provides appropriate training and guidance to support staff in fulfilling their responsibilities.

Miss Gleeson liaises with external bodies such as Network Connect and works closely with the school's technical staff to maintain a safe digital environment. She receives and logs reports of Digital Safeguarding incidents, using this information to inform future policy and practice. Regular meetings are held with the E-Safety Governor to discuss current issues, review incident logs, and examine filtering and change control records, ensuring that digital safeguarding remains a priority across the school.

ICT TECHNICIAN / NETWORK MANAGER

The ICT Technician / Network Manager plays a vital role in maintaining the safety and integrity of St Joseph's digital infrastructure. They are responsible for ensuring that the school's technical systems are secure and protected against misuse or malicious attacks. This includes ensuring that the school meets all required digital safeguarding technical standards, including any guidance provided by the Local Authority.

Access to the school's networks and devices is managed through a properly enforced password protection policy. The ICT Technician ensures that filtering systems, provided by Network Connect, are applied and regularly updated in line with school policy, and that their implementation is not the sole responsibility of any one individual.

To effectively carry out their digital safeguarding role, the ICT Technician keeps up to date with relevant technical developments and shares updates with staff as needed. They monitor the use of the school's network, internet, virtual learning environments, remote access, and email systems to identify and report any misuse or attempted misuse. Monitoring software and systems are implemented and maintained in accordance with school policies to support a safe and secure digital learning environment.

TEACHING AND SUPPORT STAFF:

Are responsible for ensuring that:

- They have an up to date awareness of Digital Safeguarding matters and of the current school Digital Safeguarding policy and practices;
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) – ***appendix 1***
- They report any suspected misuse or problem to the Headteacher ;
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems ;
- Digital Safeguarding issues are embedded in all aspects of the curriculum and other activities;
- Pupils understand and follow Digital Safeguarding and acceptable use policies;
- 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 pupils should be guided to sites checked as suitable for their use e.g. (St Josephs – Kiddle search engine) and that processes are in place for dealing with any unsuitable material that is found in internet searches.

CHILD PROTECTION / SAFEGUARDING DESIGNATED PERSON:

At St. Joseph's Catholic Primary School Wrightington, the head teacher – ***Miss Gleeson***- is the Designated Senior Lead for Safeguarding and the Assistant Headteacher – ***Mrs Porter-*** is the back-up Designated Senior Lead for Child Protection and is responsible for these things in her absence.

The child protection designated person should be trained in Digital Safeguarding 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

(***nb. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.***

PUPILS:

- They are responsible for using the school technology systems in accordance with the Pupil Acceptable Use Policy - ***appendix 2;*** these rules will be displayed in each class.
- They should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- They 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;

- They should understand the importance of adopting good Digital Safeguarding practice when using digital technologies in and out of school and children are taught about the importance of this in school Digital Literacy sessions.

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. St Joseph's will take every opportunity to help parents understand these issues through parents' evenings, assemblies, newsletters, digital leaders coffee mornings/website / Digital Safeguarding campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good Digital Safeguarding practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- comments on the blog.

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

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

- A planned Digital Safeguarding curriculum should be provided as part of Computing / PHSEE / other lessons and should be regularly revisited (St Joseph's use the Digital Literacy and Citizenship resources and these 5 lessons are covered throughout the academic year)
- Key Digital Safeguarding 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;
- 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;
- 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 (or other relevant designated person) 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.

EDUCATION – PARENTS / CARERS:

Many parents and carers have only a limited understanding of Digital Safeguarding risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
St Joseph's will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities;
- Letters, newsletters, web site;
- Parents / Carers evenings / sessions;
- High profile events / campaigns eg Safer Internet Day;
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

EDUCATION & TRAINING – STAFF / VOLUNTEERS:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal safeguarding training will be made available to staff. This will be regularly updated and reinforced. An audit of the internet safeguarding training needs of all staff will be carried out regularly;
- All new staff should receive internet safeguarding training as part of their induction programme, ensuring that they fully understand the schools internet safeguarding policy and Acceptable Use Agreements;

TRAINING – GOVERNORS:

The Internet Safeguarding Governor takes part in training sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation;
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

TECHNICAL – INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements;
- There will be regular reviews and audits of the safety and security of school technical systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school technical systems and devices;
- All users required to log in this is controlled by Technician.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader.

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by Fortigate Filter controlled by Network Connect and the school.
- Technician staff regularly monitor and record the activity of users on the school technical systems.
- Appropriate security measures are in place (via Fortigate and Sophos).
- An agreed acceptable use statement is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems;
- An agreed acceptable use policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school - ***appendix 3;***

BRING YOUR OWN DEVICE (BYOD)

People are allowed to bring in their own devices. However, they are not allowed to connect to the network.

- The school has a set of clear expectations and responsibilities for all users;
- The school adheres to the Data Protection Act principle;
- All users are provided with and accept the Acceptable Use Agreement:
- Any device loss, theft, change of ownership of the device is the responsibility of the owner NOT the school.

Cameras, Mobile Phones and Devices:

ST JOSEPH'S CATHOLIC PRIMARY SCHOOL is committed to keeping pupils safe by ensuring that electronic devices such as cameras, phones and tablets are used in an appropriate manner. School will therefore ensure that:

- parental consent is obtained to take and use photographs and/or videos of children;
- parental consent is obtained for photographs to be taken by the media for use in relation to promoting or publishing the school;
- separate parental consent is obtained if any other agency requests to take photographs of any child;
- parental consent will be valid for 7 years but may be sought more regularly at the discretion of the headteacher;
- images will be uploaded to, and stored in a secure place for a relevant amount of time, this may be for longer than the child is at school if appropriate;
- photographs and videos of children are only taken to provide evidence of their achievements for developmental records or for other school related purposes;
- staff, visitors, volunteers and students do not use their own mobile phones to take or record any images of children; unless authorised by the HT and DHT - ***appendix 4;***
- Mobile phones should only be used when children are NOT present unless in an exceptional circumstance which has been authorised by the HT- ***appendix 5;***
- the school's photographic equipment must not leave the school setting unless this is agreed by the headteacher for official school business- ***appendix 6;***

- photos are printed/uploaded in the setting by staff and once done images are immediately removed from the equipment's memory;
- parents are reminded frequently of the risks associated with posting images of children to social media; however staff may take and share images in line with the Acceptable Use Policy which has been signed by Parents;
- parents are reminded frequently that they are not permitted to distribute or post images that contain children other than their own;
- ***The Acceptable Use Policy*** will outline when and where staff, volunteers and visitors can use their mobile phones;
- ALL staff, volunteers and visitors will adhere to the above policies and failure to do so will be addressed appropriately by the headteacher and/or the Governing Body;
- DFE Advice ***'Searching, Screening and Confiscation'*** is followed where there is a need to search a pupil for a mobile device;
- If a child brings a mobile phone or electronic device into school, this will be stored in the school safe and returned to the child/parent at the end of the day.

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.

Staff must ensure that they:

- Take care at all times 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;

SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY:

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in '***The use of social networking sites and other forms of social media policy.'***

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk;

School staff should ensure that:

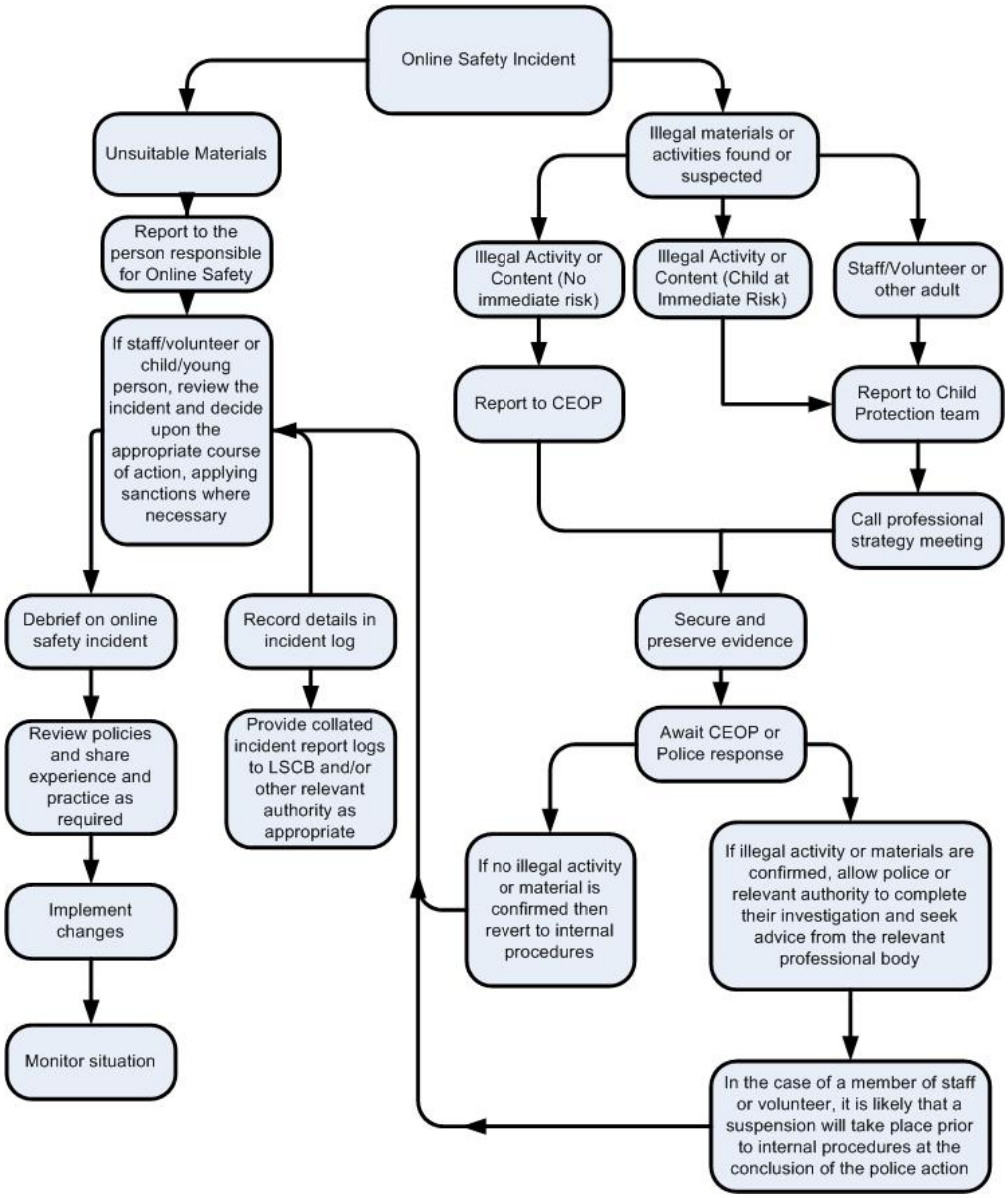
- No reference should be made in social media to pupils, parents / carers or school staff;
- They do not engage in online discussion on personal matters relating to members of the school community ;
- Personal opinions should not be attributed to the school or local authority;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes may be checked regularly by the head teacher to ensure compliance with the following policies:

- Twitter Policy
- The use of social networking sites and other forms of social media

ILLEGAL INCIDENTS:

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 (below and appendix) for responding to online safety incidents and report immediately to the police.



OTHER INCIDENTS:

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy.

SCHOOL ACTIONS & SANCTIONS:

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Appendix 1

St. Joseph's Catholic Primary, Wrightington.

Acceptable Internet Use Statement

For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school is keen to see staff make full use of the system, in order that they might broaden their skills and enhance their professional development.

The school's Internet Access Policy has been drawn up to protect all parties. Staff are reminded that inappropriate use of the internet could result in action being taken under the terms of the School's disciplinary procedure. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff and students requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the headteacher for approval.

Therefore, it is important that all staff familiarize themselves with the principles set out below-

- All Internet activity should be appropriate to staff professional activity, including research for professional purposes. Where the system is made available for personal use, the same principles apply.
- Under the terms of the Authority's Trade Union Facilities Agreement, reasonable use of computer facilities for authorised trade union representatives is permitted.
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems and laptops, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;

- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Your laptop must only be used for school related professional activity. It is not for personal use and must not be used by anyone else including family members or students.
- Files containing personal data relating to staff or students should not be held on the hard disk of your laptop, pen drives or other portable computer.
- Mobile phones must not be used to take photographs of children or of other members of staff without permission of HT (or DHT in HTs absence); however they can be used for class pictures for use on Class Dojo ***Consent form to be completed - appendix 4***
- Mobile phones should only be used when children are NOT present unless in an exceptional circumstance which has been authorised by the headteacher (or DHT in HTs absence) ***Consent form to be completed - appendix 5***
- Photographs of children or other members of staff should not be placed on any social networking sites- unless prior permission gained via The Acceptable Use Policy.

Full name : **Post:**

Signed: **Date:**

Access granted: **Date:**

Appendix 2

'Living life to the full'

Think then Click

These are our rules to keep us safe when we use digital technology at school:

- I will ask permission from a teacher before using a laptop/tablet.
- I will not access other people's files
- I will use the school laptop/tablet for my school work.
- I will not bring a memory stick into school without permission.
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher if I see something that upsets me on the screen.
- I understand that the school will monitor my use of the laptop/tablet.
- I understand that the school will check my computer files.
- I will only use my own login and password which I will keep a safe.
- I will tell a teacher if I receive a message I do not like from the laptop, tablet or e mail.
- I will always be polite and sensible when I send messages.
- I will not take my water bottle near a laptop/tablet.

I understand that if I do not follow these rules:

- My teacher will be informed
- The Head Teacher will be informed.
- My parents will be informed.
- I may be stopped from using the school laptops/ tablets.

…….. (pupil's name) agrees to follow the Online Safety rules and to support the safe use of I.C.T. at St Joseph's Catholic Primary School, Wrightington.

I confirm that I have read the school's computer rules designed to help keep my child safe.

Parent/Carer's name: …….

Signed (parent/carer): ……

Appendix 3

St. Joseph's Catholic Primary, Wrightington.

Acceptable Internet Use Statement

For Third party

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school is keen to see staff make full use of the system, in order that they might broaden their skills and enhance their professional development.

The school's Internet Access Policy has been drawn up to protect all parties. Staff are reminded that inappropriate use of the internet could result in action being taken under the terms of the School's disciplinary procedure. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff and students requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the headteacher for approval.

Therefore, it is important that all staff familiarize themselves with the principles set out below:

All Internet activity should be appropriate to staff professional activity, including research for professional purposes. Where the system is made available for personal use, the same principles apply.

Under the terms of the Authority's Trade Union Facilities Agreement, reasonable use of computer facilities for authorised trade union representatives is permitted.

Access should only be made via the authorised account and password, which should not be made available to any other person;

Activity that threatens the integrity of the school ICT systems and laptops, or activity that attacks or corrupts other systems, is forbidden;

Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;

Use for personal financial gain, gambling, political purposes or advertising is forbidden;

Copyright of materials must be respected;

Posting anonymous messages and forwarding chain letters is forbidden;

As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;

Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

Your laptop must only be used for school related professional activity. It is not for personal use and must not be used by anyone else including family members or students.

Files containing personal data relating to staff or students should not be held on the hard disk of your laptop, pen drives or other portable computer. Mobile phones must not be used to take photographs of children or of other members of staff.

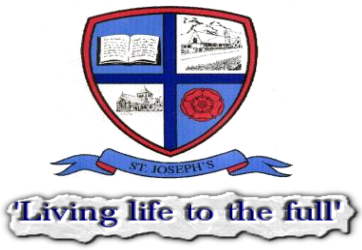
Photographs of children or other members of staff should not be placed on any social networking sites without permission from HT (or DHT in HTs absence).

Full name : **Post:**

Signed: **Date:**

Access granted: **Date:**

Appendix 4



ST. JOSEPH'S CATHOLIC PRIMARY SCHOOL, WRIGHTINGTON.

I ..... (HT/DHT) give ..... permission

to take images of children on their mobile phones and then remove them immediately

from the phones memory when they have been uploaded/printed in the school setting.

The reason for this being:_____.

Signed:_____ Designation:_____ Date:_____

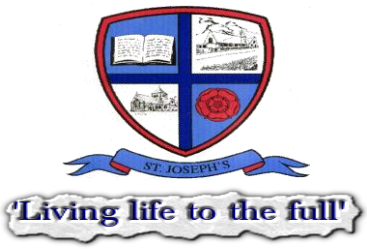
Signed:_____ Designation:_____ Date:_____

Signature of person being given permission:_____

Designation:_____

Date:_____

Appendix 5



ST. JOSEPH'S CATHOLIC PRIMARY SCHOOL, WRIGHTINGTON

I ..... (HT/DHT) authorise _____ to keep their mobile phone with them around school and in class on _____ because _____

_____

Signed:_____ Designation:_____ Date:_____

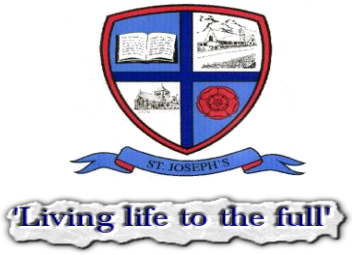
Signed:_____ Designation:_____ Date:_____

Signature of person being authorised:_____

Designation:_____

Date:_____

Appendix 6



ST. JOSEPH'S CATHOLIC PRIMARY SCHOOL, WRIGHTINGTON.

I ..... (HT/DHT) authorise _____ to

take school's photographic equipment off site on _____.

Reason:_____

Signed:_____ Designation:_____ Date:_____

Signed:_____ Designation:_____ Date:_____

Signature of person being authorised:_____

Designation:_____

Date:_____