ST. JOHN LLOYD CATHOLIC COMPREHENSIVE SCHOOL

E-Safety Policy

School Mission Statement

Learning and Growing Together in Christ

"As a Catholic School we aim to develop a Christian Community which believes in and affirms the dignity and value of the individual and encourages its members to develop their potential in terms of knowledge, understanding, spiritual, moral, cultural and physical awareness".

This policy applies to all members of the 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 the school.

Approved: 30th November 2016
Reviewed: 10th December 2020

Development / Monitoring / Review of this Policy

This e-Safety policy has been developed by the E-Safety committee at St. John Lloyd Catholic School, made up of:

- Head teacher / Senior Leaders
- e-Safety Coordinator
- Staff – including Teachers, Technical staff
- Governors

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

Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the Governing Body / Governors Sub Committee on:	30th November 2016
The implementation of this e-Safety policy will be monitored by the:	E-Safety Committee
Monitoring will take place at regular intervals:	Annually
The Governing Body / Governors Sub Committee will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	Annually
The e-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 e-Safety or incidents that have taken place. The next anticipated review date will be:	01/01/2018
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Roles and Responsibilities

The following section outlines the e-Safety roles and responsibilities of individuals and groups within the school :

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing body / Governor's Sub-committee receiving regular information about e-Safety incidents and monitoring reports. Regular meetings with the e-Safety Co-ordinator will consist of;

- regular monitoring of e-Safety incident logs
- regular monitoring of filtering / change control logs (where possible)
- reporting to relevant Governors / sub-committee

Head teacher and Senior Leaders:

- **The Head teacher has a duty of care for ensuring the safety (including e-Safety) of members of the school community**, though the day to day responsibility for e-Safety may be delegated to the e-Safety Co-ordinator.
- **The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.**
- The Head teacher and Senior Leaders are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The Head teacher 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 e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the e-Safety Co-ordinator.

e-Safety Coordinator:

The *e-Safety Coordinator:*

- leads the e-Safety committee
- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the schools e-Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with schools' technical staff
- receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.

Network Manager / Technical staff:

The Network Manager 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 the required e-Safety technical requirements as identified by the *Local Authority or other relevant body* and also the e-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**
- that the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- that they keep up to date with e-Safety 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 / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher / Senior Leader; e-Safety Coordinator for investigation / action / sanction
- that (if present) 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 e-Safety matters and of the current school e-Safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP / AUA)**
- **they report any suspected misuse or problem to the *Head teacher / Senior Leader ; e-Safety Coordinator* for investigation / action**
- **all digital communications with students / pupils / parents / carers should be on a professional level** *and only carried out using official school systems*
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-Safety and acceptable use agreements / 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

Safeguarding Designated Person:

The *Safeguarding Designated Person* should be trained in e-Safety issues and be aware of the potential for serious 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

e-Safety Group:

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

Members of the e-Safety Committee will assist the e-Safety Coordinator with:

- the production / review / monitoring of the school e-Safety policy / documents.
- the production / review / monitoring of the school filtering policy.
- mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression.
- monitoring network / internet / incident logs where possible
- consulting stakeholders – including parents / carers and the students / pupils about the e-Safety provision.
- monitoring improvement actions identified through use of the 360 degree safe Cymru self-review tool.

Students / pupils:

- **are responsible for using the school digital technology systems in accordance with the Student / 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 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

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 / VLE and information about national / local e-Safety campaigns / literature.* Parents and carers will be encouraged to support the

school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the school

Community Users:
Community Users who access school systems / website / VLE 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 – young people:
Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / 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.

"e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages accross the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:"

- **A planned e-Safety curriculum should be provided as part of ICT / Computing / PSE / Digital Literacy lessons or other lessons and should be regularly revisited**
- **Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students / 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.**
- **Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- Students / pupils should be helped to understand the need for the student / 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 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.
- Where students / 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 (e.g. 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.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities:

- **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 will be provided with a username and secure password** by the network manager *who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password**
- **The administrator passwords for the schools' ICT system, used by the Network Manager must also be available to the *Head teacher* or other nominated senior leader and kept in a secure place (e.g. school safe)**
- **The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- *The school has provided enhanced / differentiated user-level filtering*
- *Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

- *An agreed 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.*
- *An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

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 by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

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:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- 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 students / 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 will be checked regularly by the senior risk officer and e-Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Use of Cloud Services

The movement towards tablet and other mobile technologies in schools presents both opportunities as well as challenges. Ultimately, the opportunities are around teaching and learning; the challenges are around successfully managing this pedagogical shift and taking staff, parents and pupils through this technological change. At the heart of the change is a move away from devices or systems where information is stored locally, to devices which can access data stored 'in the cloud'. Just as a PC needs to be connected to a network to get to the stored data, so must these mobile and tablet devices be connected to the cloud. Wireless access provides this connection.

Software too can sit in the cloud removing the need for locally installed suites of software. Apps offer an opportunity to create low cost, flexible learning opportunities which are device agnostic and which can create personalised learning on a new level.

Schools using the Hwb+ learning platform will have been provisioned with Office 365 which offers cloud based email, calendar and storage facilities as well as MS Office. By it's nature, Office 365 is available on any device which is connected to the internet meaning that these cloud based services can be accessed in school or at home on smartphones, tablets, laptops, notebooks and PCs. Schools may wish to encourage a Bring Your Own Device (BYOD) approach which will require as a minimum a strengthening of the existing Acceptable Use Policy/Agreement.

Just as a school has obligations around data on its physical network, the same obligations are required when dealing with data in the cloud i.e. it is still required to be protected in line with the Data Protection Act (DPA) and may be subject to Freedom of Information (FOI) requests.

Office 365 – further information:

Where is the data stored?
Data for UK Schools is all hosted within the EU. The primary Microsoft data centre we host the service in is located in Dublin and the fail-over is to Amsterdam.

How often is the data backed up?
The idea of "back up" is very different with Office365 than with traditional locally hosted services. We use a network of globally redundant data centres and replicate data on multiple servers across the two data centres. Any one time we keep 3 copies of schools data across the two data-centres mentioned (Dublin & Amsterdam).

Does the email service provider have a clear process for recovering data?
Yes. Users themselves can recover data for 30 days after deleting an item. Administrators then have a further 30 days once the item is deleted from the deleted-items folder. There are also additional paid-for archiving services available with

Office365, but with a 25GB inbox per person the pressure on users to archive email is not as great compared to existing email systems.

How does the email provider protect your privacy?
3 key things: No advertising, no “mingling” of Office 365 data with our consumer services (such as Hotmail) and full data-portability, in case you ever want to leave the service.

Who owns the data that you store on the email platform?
Schools own the data. Microsoft does not. You own your data, and retain all rights, title and interest in the data you store with Office 365. You can download a copy of all of your data at any time and for any reason, without any assistance from Microsoft.

Who has access to the data?
By default no one has access to customer data within the Office 365 service. Microsoft employees who have completed appropriate background checks and have justified need can raise an escalation for time-limited access to Customer data. Access is regularly audited, logged and verified through the ISO 27001 Certification.
As detailed in a recent accreditation submission to the UK Government, any organisation that specify “UK” as their country during tenant creation will be provisioned and data stored within the EU datacenters (Dublin and Amsterdam).

Microsoft has been granted accreditation up to and including the UK government’s “Impact Level 2” (IL2) assurance for Office 365. As of February 2013 Microsoft are the only major international public cloud service provider to have achieved this level of accreditation and, indeed, it is the highest level of accreditation possible with services hosted outside of the UK (but inside of the EEA).

Schools may wish to consider the extent to which applicable laws in the US – which apply to services operated by companies registered in the US, e.g. Microsoft and Google – affect the suitability of these services. For
example the US Patriot Act provides a legal means through which law enforcement agencies can access data held within these services without necessarily needing the consent or even the knowledge of the customer. Whilst SWGfL doesn’t intend to put anyone off getting value from these beneficial services we feel it’s only right to share what we know about them.

Is personal information shared with anyone else?
No personal information is shared.

Does the email provider share email addresses with third party advertisers? Or serve users with ads?

No. There is no advertising in Office365.

What steps does the email provider take to ensure that your information is secure?

Microsoft uses 5 layers of security - data, application, host, network and physical. You can read about this in a lot more detail here.

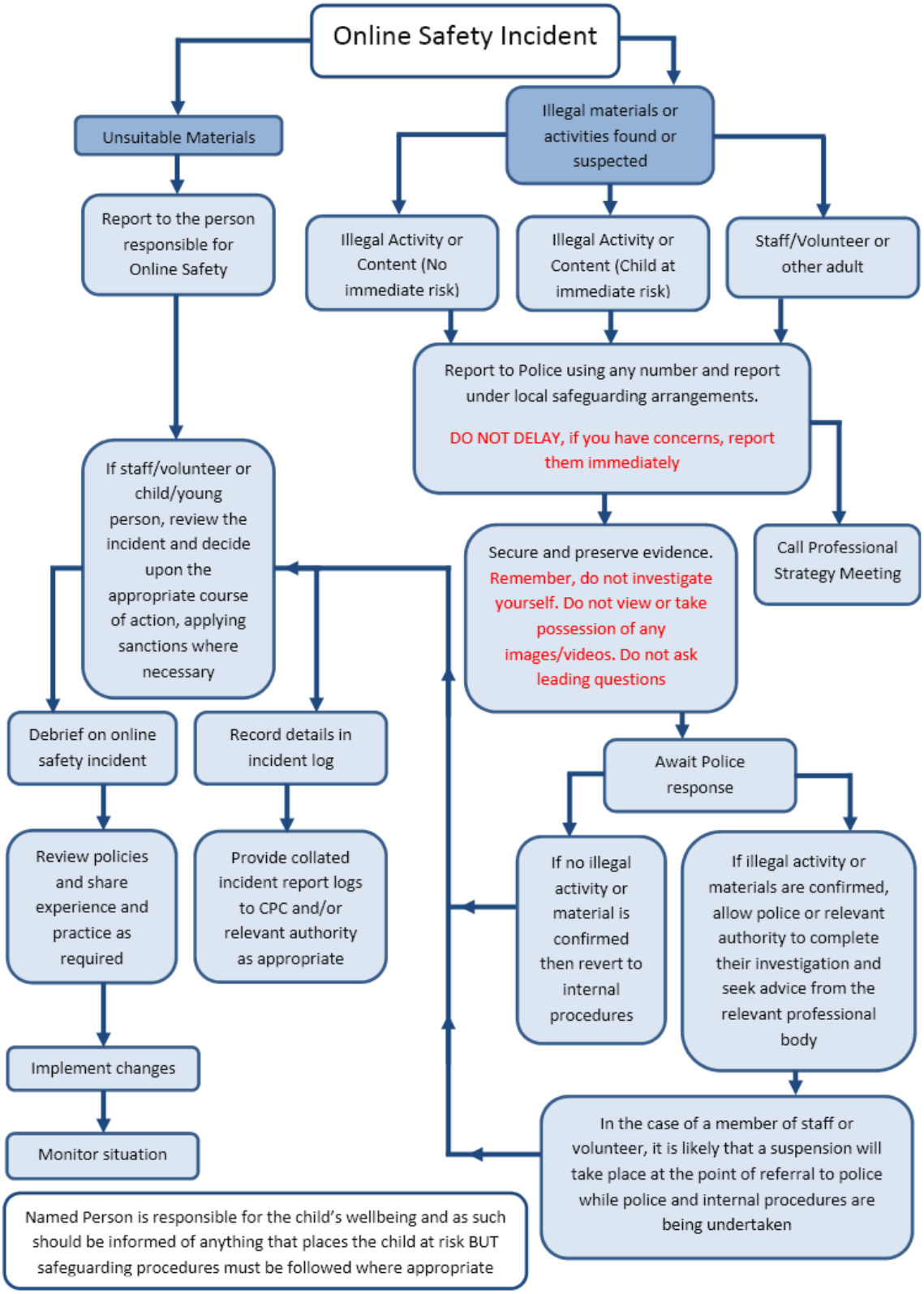
Office365 is certified for ISO 27001, one of the best security benchmarks available across the world. Office 365 was the first major business productivity public cloud service to have implemented the rigorous set of physical, logical, process and management controls defined by ISO 27001.

EU Model Clauses. In addition to EU Safe Harbor, Office 365 is the first major business productivity public cloud service provider to sign the standard contractual clauses created by the European Union ("EU Model Clauses") with all customers. EU Model Clauses address international transfer of data.

Data Processing Agreement. Microsoft offers a comprehensive standard Data Processing Agreement (DPA) to all customers. DPA addresses privacy, security and handling of customer data. Our standard Data Processing Agreement enables customers to comply with their local regulations. Visit here to get a signed copy of the DPA.

How reliable is the email service?
There is a 99.9% uptime commitment with financially-backed SLA for any paid-for services in Office365 (though most schools will be using 'free' services and therefore will not receive the financially backed SLA).

What level of support is offered as part of the service?
Microsoft offer schools direct telephone support 24/7 for IT administrators and there is also a large range of online help services, which you can read about here. Our recommendation is that schools use a Microsoft partner or support organisation with industry specific expertise in cloud services for schools.


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
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have concerns, report them immediately
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions
Call Professional Strategy Meeting
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
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
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT safeguarding procedures must be followed where appropriate

Record of reviewing devices / internet sites
(responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

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. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action
- **If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions:
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. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

St. John Lloyd Catholic
Comprehensive School
Havard Road
Llanelli
SA14 8SD

Tel: (01554) 772589
E-Mail: office@stjlloyd.carms.sch.uk
Web: www.stjohnlloyd.co.uk

ST JOHN LLOYD
CATHOLIC SCHOOL

Headteacher/Pennaeth
Mr DA Howells
BSc (Hons), NPQH

Ysgol Gyfun Gatholig
Sant Ioan Llwyd
Heol Havard
Llanelli
SA14 8SD

Ffon: (01554) 772589
E-Bost: office@stjlloyd.carms.sch.uk
Gwefan : www.stjohnlloyd.co.uk

"Learning and Growing Together in Christ"
"Dysgu ac Tyfu Gyda'n Gilydd yng Nghrist"

"As a Catholic School we aim to develop a Christian community which believes in and affirms the dignity and value of the individual and encourages its members to develop their potential in terms of knowledge, understanding, spiritual, moral, cultural and physical awareness."

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

Staff (and Volunteer) Acceptable Use Policy

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of

their policies which relate to the personal use, by staff and volunteers, of school systems)

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. (schools / academies should amend this section in the light of their policies on installing programmes / altering settings)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date:

St. John Lloyd Catholic
Comprehensive School
Havard Road
Llanelli
SA14 8SD

Tel: (01554) 772589
E-Mail: office@stjlloyd.carms.sch.uk
Web: www.stjohnlloyd.co.uk

ST JOHN LLOYD
CATHOLIC SCHOOL

Headteacher/Pennaeth
Mr DA Howells
BSc (Hons), NPQH

Ysgol Gyfun Gatholig
Sant Ioan Llwyd
Heol Havard
Llanelli
SA14 8SD

Ffon: (01554) 772589
E-Bost: office@stjlloyd.carms.sch.uk
Gwefan : www.stjohnlloyd.co.uk

"Learning and Growing Together in Christ"
"Dysgu ac Tyfu Gyda'n Gilydd yng Nghrist"

St. John Lloyd Catholic School is a caring community that aims to give every pupil regardless of background the best opportunity to succeed and achieve to their full potential. We do this by providing the appropriate challenges and support they need to gain success. Whether a pupil dreams of success academically, in the sporting field or in the world of work we are committed to supporting and helping them to achieve their goals. In this context we have invested heavily in our facilities to meet our pupils' needs.

ICT Notes

As part of the schools ongoing curriculum development, pupils' work is sometimes recorded or digitally photographed. This sometimes involves using a video camera as this provides reliable evidence of work that individual pupils' have completed and allows pupils' to clearly see their achievements. However, due to recent changes in the law we need consent for a pupils' parent or guardian to be able to continue assessing work compiled in this way. I take this opportunity to assure you that any imagery taken is used for nothing other than educational purposes and will not be made available to any other persons or agency outside the confines of St. John Lloyd Catholic School.

With the development of Information Communication Technology (ICT) within St. John Lloyd Catholic School there is a need for an **'Acceptable Use'** Policy. Pupils will be supervised during lessons and ICT related clubs and must follow the guidelines listed below;-

- Users should use the internet primarily for education purposes, although a degree of personal use is allowed to develop confidence and proficiency. However, **'undesirable'** sites are not to be accessed.

- Users should act responsibly whilst online and **NOT** post offensive messages, intentionally waste resources or flaunt copyright rules.

- Users must **NOT** use any another users' ID and password or present themselves as anybody other than their registration.

- Users must **NOT** give personal addresses, telephone/fax numbers to any person.

- Users must under **NO** circumstances view, upload or download any material which is likely to be unsuitable for school. This applies to any material of a violent, dangerous, racist or inappropriate sexual nature. Possession of certain types of material can lead to prosecution.

- Users should always respect the privacy of documents and files or any other pupil or member of staff.

If the acceptable use policy is breached, users will face disciplinary action which, in the first instance may take the form of a ban, temporary or permanent, on the use of the ICT facilities at St. John Lloyd Catholic School. If appropriate, action may also be taken in accordance with the schools' disciplinary procedures.

Users should note that the schools' access to the internet is provided by Carmarthenshire County Council LEA, where every effort is made to filter out undesirable material. However, content filtering is not 100% reliable, therefore undesirable images/content may pass through the filter. When such images/content are inadvertently displayed, the onus is on the user to report the site to the supervising member of staff and clear the screen.

User guidelines for internet and network use

Users are responsible for good behaviour on the school network and on the internet. Just as they are expected in the grounds of the school.

General school rules apply

The school network and the internet are provided for users in the school to carry out work, conduct research and communicate with others, and access is given as a privilege, not a right and access requires responsibility and compliance with general school standards.

Computer storage areas and memory devices will be treated like school lockers. Staff will review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on memory devices will always be private, and **random electronic monitoring will take place.**

The following are not permitted and will not be tolerated

- Sending, receiving or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems, computer equipment or computer networks
- Violating copyright laws
- Use of other users IDs' and passwords
- Trespassing in others' folders, work or files
- Intentionally wasting limited resources (Internet chat is not acceptable)
- Downloading or installing programmes from the internet, Removable media or any other source

Violations of the above rules will result in firm disciplinary action being taken

Sanctions

- Temporary or permanent ban on network use
- Parents will be notified
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour
- When applicable, police or local authorities may be asked to intervene

<u>This form must be signed and returned to the school and to the appropriate authority to be reviewed as approval and acceptance of the above.</u>

Pupil Name: ……

Pupil:
As a school user of ICT, I agree to comply with the school rules on its use. I will use the network in a responsible manner and observe all the restrictions to me by the school.

Pupil Signature: ……

Parent Name: ……

As the parent/guardian of the pupil signing above, I grant permission for them to use the schools ICT facilities and understand that they will be held accountable what they do. I also grant access for any photographs/videos of the above pupil to be used in the school prospectus, on the schools website, public/school displays.

Parent Signature: ……...

St. John Lloyd Catholic
Comprehensive School
Havard Road
Llanelli
SA14 8SD

Tel: (01554) 772589
E-Mail: office@stjlloyd.carms.sch.uk
Web: www.stjohnlloyd.co.uk

ST JOHN LLOYD
CATHOLIC SCHOOL

Ysgol Gyfun Gatholig
Sant Ioan Llwyd
Heol Havard
Llanelli
SA14 8SD

Ffon: (01554) 772589
E-Bost: office@stjlloyd.carms.sch.uk
Gwefan : www.stjohnlloyd.co.uk

Headteacher/Pennaeth
Mr DA Howells
BSc (Hons), NPQH

"Learning and Growing Together in Christ"
"Dysgu ac Tyfu Gyda'n Gilydd yng Nghrist"

"As a Catholic School we aim to develop a Christian community which believes in and affirms the dignity and value of the individual and encourages its members to develop their potential in terms of knowledge, understanding, spiritual, moral, cultural and physical awareness."

St. John Lloyd Catholic School is a caring community that aims to give every pupil regardless of background the best opportunity to succeed and achieve to their full potential. We do this by providing the appropriate challenges and support they need to gain success. Whether a pupil dreams of success academically, in the sporting field or in the world of work we are committed to supporting and helping them to achieve their goals. In this context we have invested heavily in our facilities to meet our pupils' needs.

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name

Signed

Date