|  |
| --- |
| [School Logo](https://www.stilltydsschool.co.uk/) |
| **E-Safety Policy** |
| At Saint Illtyd’s with God’s love we play, learn and grow together |

# SCHOOL DETAILS

**Name**: St Illtyd’s Primary School

**Address**: Jersey Road,

Bon-y-Maen

Swansea

SA1 7DG

**Head Teacher**: Mrs Maria Davies

**Web**: https://www.stilltydsschool.co.uk/

**Email**: [St.Illtyds.School@swansea-edunet.gov.uk](mailto:St.Illtyds.School@swansea-edunet.gov.uk)

**Phone**: 01792 462104

DOCUMENT VERSION CONTROL

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Purpose/Change** | **Author** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Next review date – ANNUAL REVIEWS** | | | |

Policy agreed by Governors:

….………………………………………….………………… (Signed by Chair)

………………………………………………. Date





Online Safety Policy Template for schools and colleges

# Introduction

The online safety policy template

These school/college online safety policy templates are intended to help school/college leaders produce a suitable online safety policy document which will consider all current and relevant issues, in a whole school/college context, linking with other relevant policies, such as the safeguarding, behaviour and anti-bullying policies.

The requirement to ensure that learners are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools/colleges are bound. Schools/colleges must, through their online safety policy, meet their statutory obligations to ensure that learners are safe and are protected from potential harm, both on and off-site. The policy will also form part of the school’s/college’s protection from legal challenge, relating to the use of digital technologies.

These policy templates suggest policy statements which, in the view of Welsh Government, would be essential in any school/college online safety policy, based on good practice. In addition there are a range of alternative statements that schools/colleges should consider and choose those that are most suitable, given their particular circumstances.

An effective school/college online safety policy must be tailored to the needs of each school/college and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole school/college community.

It is suggested that consultation in the production of this policy should involve:

* Governors
* Teaching staff and support staff
* Learners
* Community users and any other relevant groups.

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

Schools/colleges are subject to an increased level of scrutiny of their online safety practices by

Estyn Inspectors during inspections. From 2015 there are additional duties under the Counter Terrorism and Securities Act 2015 which requires schools/colleges to ensure that children are safe from terrorist and extremist material on the internet.

Given the range of optional statements offered and the guidance notes provided, this template document is much longer than the resulting policy is likely to be. It is intended that, while covering a complicated and ever changing aspect of the work of the school/college, the resulting policy should be concise and easily understood, if it is to be effective and adopted by all.

The template uses a number of alternative terms, e.g. school/college, these need to be deleted as relevant.

Within this template sections which include information or guidance are shown in **BLUE**. It is anticipated that schools/colleges would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

**Where sections are highlighted in BOLD text, it is strongly suggested that these should be an essential part of a school/college online safety policy.**

*Where sections in the template are written in ITALICS it is anticipated that schools/colleges would wish to carefully consider whether or not to include that section or statement in their completed policy.*

The first part of this document (approximately 25 pages) provides a template for an overall online safety policy for the school/college. The appendices contain acceptable use agreement templates and more detailed, specific policy templates. It will be for schools/colleges to decide which of these documents they chose to amend and adopt.

St Illtyd’s Primary School

E-Safety Policy

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

# Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group/committee made up of: K. Powell, J. Evans and S. Lynch.

* *Headteacher/senior leaders*
* *Online safety officer/coordinator*
* *Staff – including practitioners//support staff/technical staff*
* *Governors*
* *Parents and carers*
* *Community users*

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

### Schedule for Development/Monitoring/Review

|  |  |
| --- | --- |
| This online safety policy was approved by the *Governing body on:* |  |
| The implementation of this online safety policy will be monitored by: | *Mrs A. Heald (Head Teacher)*  *Mrs M. Davies (Deputy Head Teacher)*  *Mr S. Lynch (ICT Technician)*  *Miss J. Evans (ICT Subject Leaders)*  *Governors* |
| Monitoring will take place at regular intervals: | *Once a year.* |
| The *Governing Body/governors subcommittee* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | *Once a year.* |
| The online 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 online safety or incidents that have taken place. The next anticipated review date will be: | *March 2019* |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | *City and County of Swansea ICT*  *LA* |

The school will monitor the impact of the policy using: *(delete/add as relevant)*

* *Logs of reported incidents*
* *Monitoring logs of internet activity (including sites visited)* If possible – may need the
* *Internal monitoring data for network activity* assistance of service
* *Surveys/questionnaires of* provider
  + *Learners*
  + parents and carers
  + *staff*

# Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals[[1]](#footnote-1)and groups within the school:

Governors:

Governorsare responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the G*overning Body* receiving regular information about online safety incidents and monitoring reports. A member of the Governing Bodyshould take on the role of online safety governor[[2]](#footnote-2) toinclude:

* regular meetings with the online safety co-ordinator/officer
* reporting to relevant governors/sub-committee/meeting

Headteacher and senior leaders:

* The headteacherhas a duty of care for ensuring the safety (including online safety) of members of the school/college community, though the day to day responsibility for online safety may be delegated to the ICT Technician and ICT subject leader.
* The headteacher and deputy headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff**[[3]](#footnote-3)**
* The headteacher is responsible for ensuring that the online safety co-ordinator/officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
* The headteacher and deputy headteacher will ensure that there is a system in place to allow for monitoring and support of those in school/college who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
* The headteacher will receive regular monitoring reports from the online safety coordinator/officer.

Online safety co-ordinator/officer:

The online safety co-ordinators*/officers*

* leads the online safety group
* takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school/college online safety policies/documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* provides (or identifies sources of) training and advice for staff
* liaises with the local authority/relevant body
* liaises with (school/college) technical staff
* receives reports of online safety incidents[[4]](#footnote-4) and creates a log of incidents to inform future online safety developments.
* meets with online safety governor to discuss current issues, review incident logs and if possible, filtering change control logs
* attends relevant meeting/sub-committee of governors
* reports regularly to headteacher/senior leadership team

Network manager/technical staff:

NOTE: If the school/college has a managed ICT service provided by an outside contractor, it is the responsibility of the school/college to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school/college technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school/college online safety policy and procedures.

Thenetwork manager/technical staff(or managed service provider) is responsible for ensuring:

* that the *school/college* technical infrastructure is secure and is not open to misuse or malicious attack
* that the school/collegemeets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body and also the online safety policy/guidance that may apply.
* that users may only access the networks and devices through a properly enforced password protection policy.
* that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
* that the use of the *network/internet/learning platform/Hwb/remote access/email* is regularly monitored in order that any misuse/attempted misuse can be reported to the *headteacher/senior leader; online safety co-ordinator* for investigation/action/sanction
* *that (if present) monitoring software/systems are implemented and updated as agreed in school/college policies*

Teaching and Support Staff

Are responsible for ensuring that:

* they have an up to date awareness of online safety matters and of the current school/collegeonline safety policy and practices
* they have read, understood and signed the staff acceptable use agreement (AUA)
* they report any suspected misuse or problem to the headteacher, deputy headteacher, technician and coordinatorfor investigation/action
* all digital communications with learners/parents and carers should be on a professional level *and only carried out using official school/college systems*
* Online safety issues are embedded in all aspects of the curriculum
* Learners understand and follow the pupil promise and online safety guidance taught through citizenship lessons
* learners have an 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/college activities (where allowed) and implement current policies with regard to these devices
* in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*

### Designated senior person (Headteacher and Deputy Headteacher)

NOTE: It is important to emphasise that these are safeguarding issues, not technical issues; the technology provides additional means for safeguarding issues to develop. Some schools/colleges may choose to combine the role of designated senior person and online safety officer.

Thedesignated senior personshould be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

* sharing of personal data[[5]](#footnote-5)
* access to illegal/inappropriate materials
* inappropriate online contact with adults/strangers
* potential or actual incidents of grooming
* cyber-bullying

If the roles of the designated senior person and the online safety officer are not combined, it is suggested that they work in collaboration due to the safeguarding issues often related to online safety.

### Online safety group

The online safety group[[6]](#footnote-6) provides a consultative group that has wide representation from the school/collegecommunity, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school/college this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body*.*

Members of the online safety group (or other relevant group) will assist the online safety coordinator/officer (or other relevant person, as above) with:

* the production/review/monitoring of the school/college online safety policy/documents.
* *the production/review/monitoring of the school/college filtering policy (if possible and if the school/college chooses to have one) and requests for filtering changes.*
* mapping andreviewing the online safety curricular provision – ensuring relevance, breadth and progression
* monitoring network/internet/incident logs where possible
* consulting stakeholders – including parents/carers and the learners about the online safety provision
* monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

An online safety group terms of reference template can be found in the appendices

Learners:

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

### Parents and carers

Parents and 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/college will take every opportunity to help parents understand these issues through *parents’ evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support the school/college in promoting good online safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken at school/college events
* access to parents’ sections of the website, Hwb, learning platform and online learner records
* their children’s personal devices in the school/college (where this is allowed)

### Community Users

Community users who access school/college systems/website/Hwb/learning platform as part of the wider school/college provision will be expected to sign a community user AUA before being provided with access to school/college systems.

## Policy Statements

#### Education – learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school/college’s online safety provision. Learners need the help and support of the school/college to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: (Note: statements will need to be adapted, depending on school/college structure and the age of the learners)

* **A planned online safety curriculum across a range of subjects, (e.g. ICT/PSE/ /DCF) and topic areas and should be regularly revisited**
* **Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities**
* **Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.**
* **Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
* Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they

can influence and participate in decision-making. Nb. additional duties for schools/colleges under the Counter Terrorism and Securities Act 2015 which requires schools/colleges to ensure that children are safe from terrorist and extremist material on the internet.

* *Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/college*
* *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 learners 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 learners 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 nominated 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 and carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children’s online 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.

The school/college will therefore seek to provide information and awareness to parents and carers through: (select/delete as appropriate)

* *Curriculum activities*
* *Letters, newsletters, web site, learning platform, Hwb*
* *Parents and carers evenings/sessions*
* *High profile events/campaigns, e.g. Safer Internet Day*
* *Reference to the relevant web sites/publications, e.g.* <https://hwb.wales.gov.uk/>[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)  <http://www.childnet.com/parents-and-carers>(see appendix for further links/resources)

#### Education and training – staff/volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select/delete as appropriate)

* **Staff will receive information about online safety linked to this policy and curriculum delivery through workshops, upskilling sessions and ADDS sessions.**
* *The online safety team will receive regular updates through attendance at external training events, (e.g. from Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
* *This online safety policy and its updates will be presented staff and they will sign in agreement once read.*
* *The online safety team will provide advice/guidance/training to individuals as required.*

#### Training – governors

**Governors should take part in online safety training/awareness sessions**, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways:

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

#### Technical – infrastructure/equipment, filtering and monitoring

If the school/college has a managed ICT service provided by an outside contractor, it is the responsibility of the school/college to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school/college, as suggested below. It is also important that the managed service provider is fully aware of the school/college online safety policy/acceptable use agreements. The school/college should also check their local authority/other relevant body policies on these technical issues if the service is not provided by the authority.

The school/college will be responsible for ensuring that the school/college 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 online safety responsibilities.

**School/college technical systems will be managed in ways that ensure that the school/college meets recommended technical requirements**

* There will be regular reviews and audits of the safety and security of school/college 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/college technical systems and devices.
* All users will be provided with a username and secure password by the ICT technician *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 “master/administrator” passwords for the school/college digital systems, used by the network manager (or other person) must also be available to the headteacher and kept in a secure place, (e.g. school/college safe)
* The ICT technician 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.
* There is a clear process in place to deal with requests for filtering changes. The ICT technician is notified by the member of staff. *The school/college has (if possible) provided enhanced/differentiated user-level filtering* (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.) *through user accounts.*
* Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. N.b. additional duties for schools/colleges under the Counter Terrorism and Securities Act 2015 which requires schools/colleges to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on “appropriate filtering”).
* Where possible, school/college technical staff regularly monitor and record the activity of users on the school/college technical systems and users are made aware of this in the acceptable use agreement. (schools/colleges may wish to add details of the monitoring programmes that are used).
* An appropriate system is in place, through use of a google form, 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/college systems and data. These are tested regularly. The school/college infrastructure and individual workstations are protected by up to date virus software.
* All temporary users are required to sign the school code of conduct.
* All users of school devices for personal use are required to sign the code of conduct and will sign the loan of equipment register.
* All users of removable media (eg memory sticks/CDs/DVDs) on school/college devices should sign the school code of conduct.

## Mobile technologies

Mobile technology devices may be school/college owned/provided, might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school’s/college’s wireless network. The device then has access to the wider internet which may include the school/college learning platform and other cloud based services such as email and data storage. Personally owned devices do not access the school network unless permitted by the technician and head teacher.

All users should understand that the primary purpose of the use of mobile/personal devices in a school/college context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school/college’s online safety education programme.

 The school/college acceptable use agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies

#### Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school/college will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

**When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, eg., on social networking sites.**

* In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school/college events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, it is advised that these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images.
* *Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/college code of conduct concerning the sharing, distribution and publication of those images.*
* *Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school/college into disrepute.*
* *Learners must not take, use, share, publish or distribute images of others without their permission.*
* *Photographs published on the website, or elsewhere that include learners will be selected carefully.*
* *Learners’ full names will not be used anywhere in association with photographs.*

*on a website or blog.*

*Written permission from parents or carers about use of photographs and videos is obtained through consent pages in the home school diary.*

|  |  |
| --- | --- |
| Personal data will be recorded, processed, transferred and made available according to the | |
| current data protection legislation. |  |

The school/college must ensure that:

* it has a Data Protection Policy.
* it implements the data protection principles and is able to demonstrate that it does so.
* it has paid the appropriate fee Information Commissioner’s Office (ICO)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| \* it has appointed an appropriate Data Protection Officer (DPO) who has a high level of | | | | | |
| understanding of data protection law and is free from any conflict of interest. The | | |  | | |
| school/college may also wish to appoint a Data Manager and Systems Controllers to | | | |  | |
| support the DPO |  | | |
| \* it has an ‘information asset register’ in place and knows exactly what personal data it | | | | |
| holds, where, why and which member of staff has responsibility for managing it | |  | | |

* the information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed

|  |  |  |
| --- | --- | --- |
| \* it will hold the minimum personal data necessary to enable it to perform its function and | | |
| it will not hold it for longer than necessary for the purposes it was collected for. The | |  |
| school should develop and implement a ‘retention schedule” to support this |  |

* data held must be accurate and up to date where this is necessary for the purpose you hold it for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
* it provides staff, parents, volunteers, teenagers and older children with information about how the school / college looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
* procedures must be in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them
* data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
* IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

|  |  |
| --- | --- |
| \* it has undertaken appropriate due diligence and has GDPR compliant contracts in place | |
| with any data processors |  |

* it understands how to share data lawfully and safely with other relevant data controllers.

In Wales, schools and colleges should consider using the Wales Accord on Sharing

Personal Information toolkit to support regular data sharing between data controllers

* there are clear and understood policies and routines for the deletion and disposal of data \* it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| affected as required by law. In order to do this it has a policy for reporting, logging, | | | | |
| managing, investigating and learning from information risk incidents. | | |  | |
| \* If a maintained school/college, it must have a Freedom of Information Policy which sets | | | | | | |
| out how it will deal with FOI requests. |  | | | | | |
| \* all staff receive data protection training at induction and appropriate refresher training | | | | | |
| thereafter. Staff undertaking particular data protection functions, such as handling | | | |  | |
| requests under the individual’s rights, will receive training appropriate for their function | | | | | |
| as well as the core training provided to all staff. | |  | | | |

The school/college must ensure that:

* + It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
  + Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
  + All personal data will be fairly obtained in accordance with the privacy notice and lawfully processed in accordance with the conditions for processing. (see privacy notice section in the appendix)
  + It has a data protection policy (see appendix for policy template)
  + It is registered as a data controller for the purposes of the Data Protection Act (DPA)
  + Responsible persons are appointed/identified - senior information risk officer (SIRO) and information asset owners (IAOs)
  + Risk assessments are carried out
  + It has clear and understood arrangements for the security, storage and transfer of personal data
  + Data subjects have rights of access and there are clear procedures for this to be obtained
  + There are clear and understood policies and routines for the deletion and disposal of data
  + There is a policy for reporting, logging, managing and recovering from information risk incidents
  + There are clear data protection clauses in all contracts where personal data may be passed to third parties

**Staff must ensure that they**:

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

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

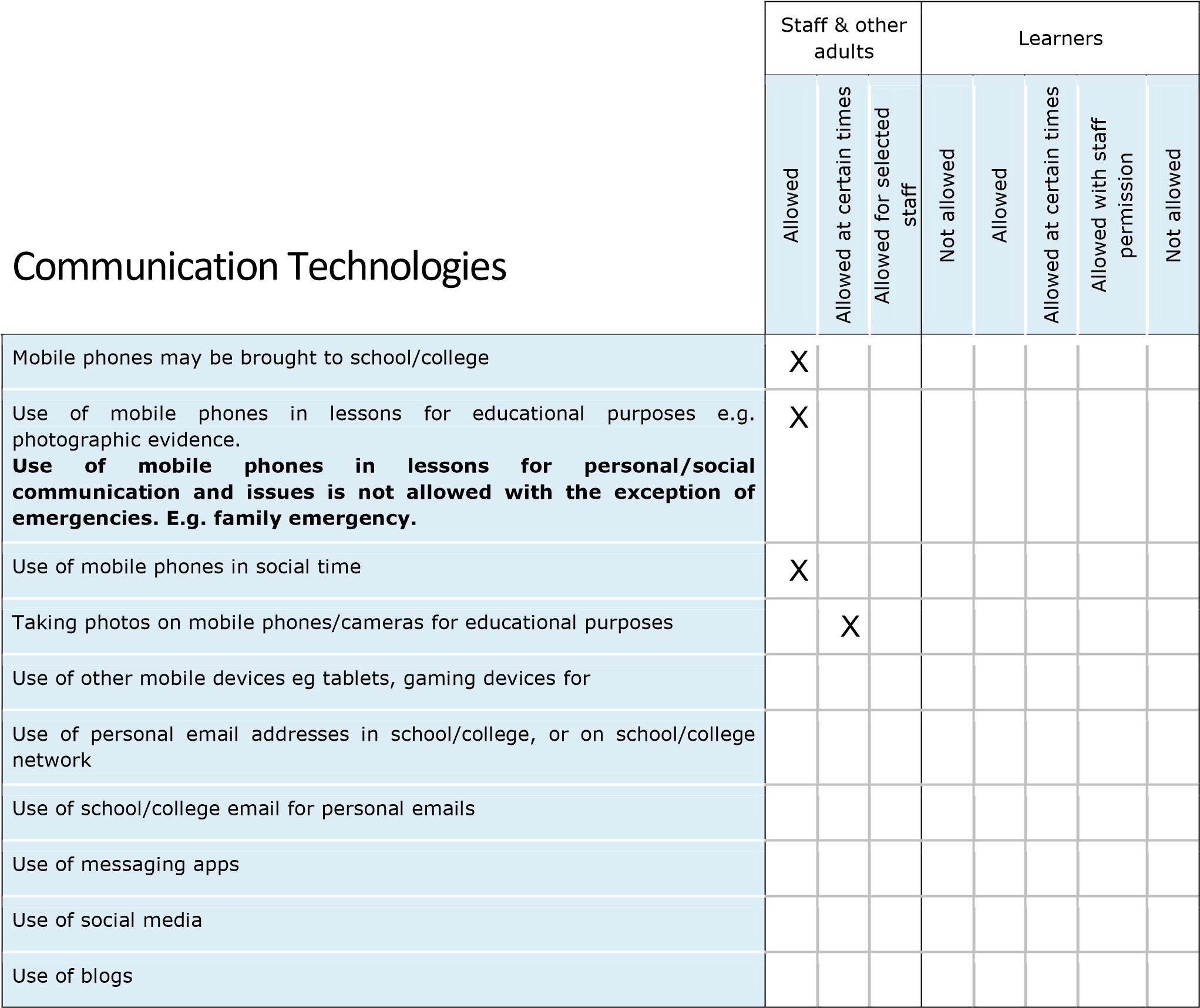
* + the data must be encrypted and password protected
  + the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
  + the device must offer approved virus and malware checking software
  + the data must be securely deleted from the device, in line with school/college policy

(below) once it has been transferred or its use is complete

#### Communications

This is an area of rapidly developing technologies and uses. Schools/colleges will need to discuss and agree how they intend to implement and use these technologies, e.g. few schools/colleges allow learners to use mobile phones in lessons, while others identify educational potential and allow their use. This section may also be influenced by the age of the learners. The table has been left blank for school/college to choose its own responses.

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



The school/college may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

When using communication technologies the school/college considers the following as good practice:

* **The official school/college email service may be regarded as safe and secure and is monitored.**
* **Users must immediately report to the online safety team – in accordance with the school/college policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
* **Any digital communication between staff and learners or parents/carers (email, chat, learning platform, etc.) must be professional in tone and content.** *These communications may only take place on official (monitored) school/college systems. Personal email addresses, text messaging or social media must not be used for these communications.*
* *Learners should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
* *Personal information should not be posted on the school/college website.*

#### Social media

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 learners, the school/college 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/colleges and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/colleges 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/college 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 learners and their families and for colleagues and the learning setting.

The school/college provides the following measures to ensure reasonable steps are in place to minimise risk of harm to through:

* Ensuring that personal information is not published
* Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
* Clear reporting guidance, including responsibilities, procedures and sanctions

School/college staff should ensure that:

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

When official school/college social media accounts are established there should be:

* A process for approval by senior leaders
* Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
* Systems for reporting and dealing with abuse and misuse
* Understanding of how incidents may be dealt with under school/college disciplinary procedures

Monitoring of Public Social Media

* Public postings about the school/college are reported to the headteacher.

#### Unsuitable/inappropriate activities

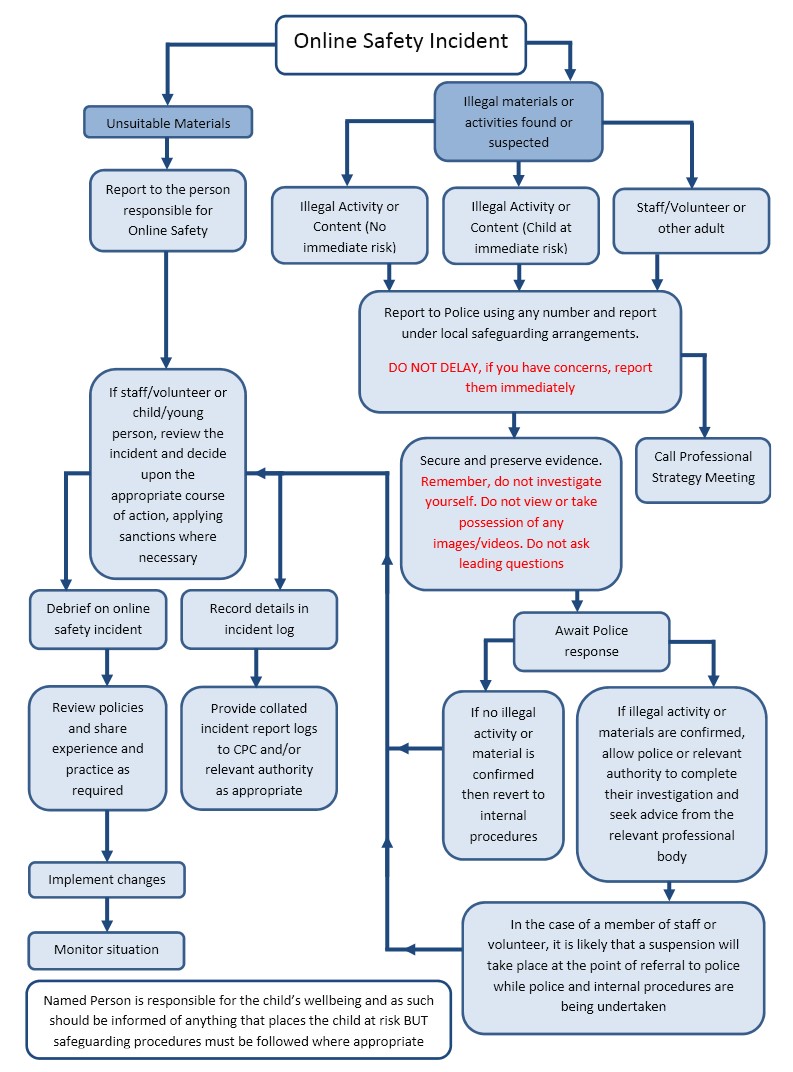
 All sites deemed unsuitable and inappropriate are blocked the school firewall and LA ICE support.

## Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

#### 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.



**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 learners 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
  + promotion of terrorism or extremism
  + 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/college 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/college actions

It is more likely that the school/college 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/college 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.

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

[https://hwb.wales.gov.uk](https://hwb.wales.gov.uk/)

### Acknowledgements

**Welsh Government and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this school/college online safety policy templates and of the 360 degree safe Cymru online safety self review tool:**

* Members of the SWGfLonline safety group
* Representatives of SW local authorities
* Representatives from a range of Welsh schools/colleges involved in consultation and pilot groups
* Plymouth University online safety

Copyright of these policy templates is held by SWGfL. Schools/colleges and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (esafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in December 2016. However, SWGfL cannot guarantee it’s accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2017

1. In a small school/college some of the roles described below may be combined, though it is important to ensure that there is sufficient “separation of responsibility” should this be the case. [↑](#footnote-ref-1)
2. It is suggested that the role may be combined with that of the Safeguarding Governor [↑](#footnote-ref-2)
3. see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant *Local Authority HR/other relevant body* disciplinary procedures. [↑](#footnote-ref-3)
4. The school/college will need to decide how these incidents will be dealt with and whether the investigation/action will be the responsibility of the Online safety co-ordinator/officer or another member of staff, e.g. headteacher/senior leader/designated senior person/class teacher/head of year etc. [↑](#footnote-ref-4)
5. See Personal Data Policy in the Appendix [↑](#footnote-ref-5)
6. School/colleges will need to decide the membership of the online safety group. It is recommended that the group should include representation from learners and parents/carers.

   [↑](#footnote-ref-6)