Ysgol Gynradd **Llanidloes** Primary School

# e-Safety Policy

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

This policy was adopted on 27th March 2017

Signed: _____ (Chair of Governing Body)

Signed: _____ (Headteacher)

Reviewed: 21st March 2018, 30th January 2019, 24th June 2020, 12th October 2022, 27th September 2023

**Contents**

- C4 School Training Needs Audit
- C5 Summary of Legislation
- C6 Office 365 – further details
- C7 Links to other organisations and documents
- C8 Glossary of terms

## Introduction

This policy aims to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely as part of the wider duty of care to which all who work in schools are bound. Schools must, through their e-Safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

## Development, Monitoring and Review of this Policy

This e-Safety policy has been developed by the e-Safety group made up of:

- headteacher
- e-Safety coordinator
- staff – including teachers and support staff
- governors
- learners
- parents and carers

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

## Schedule for Development, Monitoring and Review

| | |
|---|---|
| This e-Safety policy was approved by the Governing Body on: | 27th March 2017 |
| The implementation of this e-Safety policy will be monitored by the: | e-Safety coordinator, e-Safety group, Senior Leadership Team |
| Monitoring will take place at regular intervals: | Annually |
| The Governing Body 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: | At least 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: | Autumn 2024 |
| Should serious e-Safety incidents take place, the following external persons / agencies should be informed: | LA ICT Manager, LA Safeguarding Officer, Ceredigion ICT Manager, Police as applicable |

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
  - ✓ learners
  - ✓ parents and carers
  - ✓ staff

**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 receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body will take on the role of e-Safety governor to include:

- regular meetings with the e-Safety coordinator;
- regular monitoring of e-Safety incident logs;
- reporting to the relevant Governing Body or committee meeting.

***Headteacher and Senior Leadership Team (SLT)***

- The Headteacher 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 has been delegated to the e-Safety coordinator;
- The Headteacher and members of the SLT 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 Headteacher and SLT 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 SLT will receive regular monitoring reports from the e-Safety coordinator.

***e-Safety Coordinator***

- accounts directly to the Headteacher;
- leads the e-Safety group;
- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies and 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 (LA);
- liaises with technical staff;

- receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments;
- meets regularly with e-Safety governor to discuss current issues, review incident logs and if possible, filtering and change control logs;
- attends relevant Governing Body meetings and committees;
- reports regularly to SLT.

***Technical staff***

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

The Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets (as a minimum) the required e-Safety technical requirements as identified by the LA and also the e-Safety Policy and 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 and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or e-Safety coordinator for investigation and action or sanction;
- that monitoring software and 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 Agreement;
- they report any suspected misuse or problem to the Headteacher or e-Safety coordinator for investigation and action;
- all digital communications with learners and parents and 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;
- learners understand and follow the e-Safety and acceptable use agreements and policies;

- learners 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 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.

***Safeguarding Designated Senior Person (DSP)***

NOTE: It is important to emphasise that these are safeguarding issues, not technical issues; that the technology provides additional means for safeguarding issues to develop. Some schools may choose to combine the role of DSP and e-Safety Officer.

The Safeguarding DSP 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 or inappropriate materials;
- inappropriate on-line contact with adults or 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. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the e-Safety Group will assist the e-Safety coordinator with:

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

***Learners***

- are responsible for using the school digital technology systems in accordance with the Learner Acceptable Use Agreement;

- will 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 and 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 and Carers***

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and VLE and information about national and local e-Safety campaigns and 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 school website and VLE and on-line learner records;
- their children's personal devices in the school (where this is allowed).

***Community Users***

Community Users who access school systems, website or VLE as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement 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 learners to take a responsible approach. The education of learners 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 is a focus in all areas of the curriculum and staff will reinforce e-Safety messages across the curriculum. The e-Safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-Safety curriculum is provided as part of ICT, Computing, PSE and/or Digital Literacy and will be regularly revisited;
- Key e-Safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities;
- Learners will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information;

- Learners will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Learners will 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;
- Staff will 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, learners may need to research topics (for example, racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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 e-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities;
- Letters, newsletters, website, VLE;
- Parents' evenings and sessions;
- High profile events and campaigns (for example, Safer Internet Day);
- Reference to the relevant web sites and publications (for example, https://hwb.wales.gov.uk/; www.saferinternet.org.uk/; http://www.childnet.com/parents-and-carers).

***Education and Training – Staff and Volunteers***

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

- A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-Safety as a training need within the performance management process;
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Agreements;

- The e-Safety coordinator will receive regular updates through attendance at external training events (for example, from Consortium, SWGfL, LA and other relevant organisations) and by reviewing guidance documents released by relevant organisations;
- This e-Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days;
- The e-Safety coordinator will provide advice. guidance and training to individuals as required.

***Training – Governors***

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

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

**Technical – Infrastructure and Equipment, Filtering and Monitoring**

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-Safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school e-Safety Policy and Acceptable Use Agreements. The school should also check their LA policies on these technical issues if the service is not provided by the LA.

The school will be responsible for ensuring that the school infrastructure and 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.

**Bring Your Own Device (BYOD)**

Learners may not bring their own devices for use in school.

A device may be a privately owned smartphone, smart watch, tablet, notebook, laptop or other new technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet including the school's learning platform (Hwb) and other cloud-based services such as email and data storage. The device may typically also be used for the taking of images, for the recording of sounds or video and for generating and storing a wide range of other types of data (often as a result of using an app).

**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 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, for example, on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents and carers comment on any activities involving other learners in the digital or video images.
- Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow the school policies concerning the sharing, distribution and publication of those images. These images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital or video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school 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 and will comply with good practice guidance on the use of such images.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of learners are published on the school website.
- Learner's work can only be published with the permission of the learner and parents or carers.

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- only transferred to others with adequate protection.

The school 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";
- it has a Data Protection Policy;
- it is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
- responsible persons are appointed and 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;
- there are clear policies about the use of cloud storage and cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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 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 or any other removable media:

- the data must be encrypted and password protected;
- the device must 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 policy, once it has been transferred or its use is complete.

**Communications**

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

| | Staff and other adults | | | | Learners | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed for selected learners | Not allowed |
| Personal mobile phones may be brought to school | x | | | | | | | x |
| Use of personal mobile phones in lessons | | | | x | | | | x |
| Use of personal mobile phones in social time | x | | | | | | | x |
| Taking photos on personal mobile phones / cameras | | | | x | | | | x |
| Use of other personal mobile devices eg tablets, gaming devices | | x | | | | | | x |
| Use of personal email addresses in school, or on school network | | | | x | | | | x |
| Use of school email for personal emails | | | | x | | | | x |
| Use of messaging apps on personal devices | | x | | | | | | x |
| Use of social media on personal devices | | x | | | | | | x |
| Use of blogs on personal devices | | x | | | | | | x |

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and learners should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access);
- Users must immediately report to the nominated person - in accordance with the school 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 and carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications;
- All learners will be provided with an email address through Hwb;
- Learners will be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They will be taught strategies to deal with inappropriate

communications and be reminded of the need to communicate appropriately when using digital technologies;
- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff.

**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 learners, 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 learners 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 learners 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 learners, 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 learners, parents and 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 group to ensure compliance with the relevant policies.

## Unsuitable and Inappropriate Activities

Some internet activity, for example, accessing child abuse images or distributing racist material, is illegal and would obviously be banned from school and all other technical systems. Other activities, for example, cyber-bullying, would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

## User Actions

| | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| **Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:** | **Child sexual abuse images – the making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978;** | | | | | x |
| | **Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003;** | | | | | x |
| | **Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008;** | | | | | x |
| | **Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986;** | | | | | x |
| | **Pornography;** | | | | x | |
| | **Promotion of any kind of discrimination;** | | | | x | |
| | **Threatening behaviour, including promotion of physical violence or mental harm;** | | | | x | |
| | **Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** | | | | x | |
| **Using school systems to run a private business** | | | | | x | |
| **Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school** | | | | | x | |

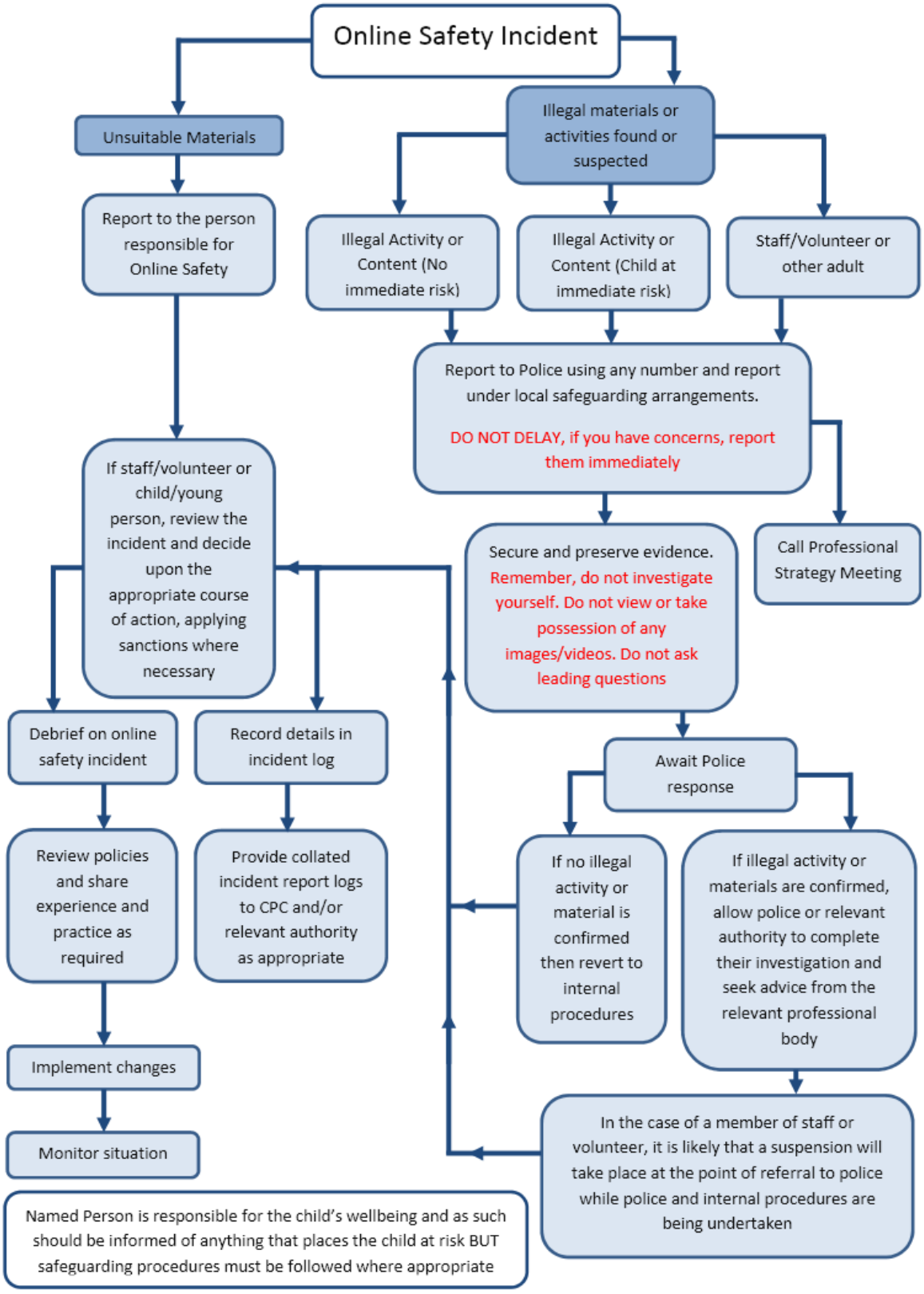
| | | | | | |
|---|---|---|---|---|---|
| **Infringing copyright** | | | | x | |
| **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)** | | | | x | |
| **Creating or propagating computer viruses or other harmful files** | | | | x | |
| **Unfair usage (downloading / uploading large files that hinders others in their use of the internet)** | | | | x | |
| **On-line gaming (educational)** | | | x | | |
| **On-line gaming (non-educational)** | | | | x | |
| **On-line gambling** | | | | x | |
| **On-line personal shopping / commerce** | | | | x | |
| **File sharing** | | | x | | |
| **Use of social media** | | | x | | |
| **Use of messaging apps** | | | x | | |
| **Use of video broadcasting eg Youtube** | | | x | | |

## 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.


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

**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 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 LA 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 and disciplinary procedures as follows.

**Learners**

| Incidents: | Refer to class teacher | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable and inappropriate activities) | | x | x | | x | | | |
| Unauthorised use of non-educational sites during lessons | x | | | | | | | |
| Unauthorised use of mobile phone / digital camera / other mobile device | | x | | | x | | | |
| Unauthorised use of social media / messaging apps / personal email | | x | | | | | | |
| Unauthorised downloading or uploading of files | | x | | | | | | |
| Allowing others to access school network by sharing username and passwords | | x | | | | | | |
| Attempting to access or accessing the school network, using another learner's account | | x | | | | | | |
| Attempting to access or accessing the school network, using the account of a member of staff | | x | | | | | | |
| Corrupting or destroying the data of other users | | x | | | | | | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | x | | | x | | | |
| Continued infringements of the above, following previous warnings or sanctions | | x | | | x | x | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | x | | | x | | | |
| Using proxy sites or other means to subvert the school's filtering system | | x | | | | | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | x | | | x | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | x | | | x | x | | |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | | x | | | | | | |

**Staff**

| Incidents: | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities) | x | x | x | | | | |
| Inappropriate personal use of the internet / social media / personal email | x | | | | | | |
| Unauthorised downloading or uploading of files | x | | | | x | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | x | | | | x | | |
| Careless use of personal data eg holding or transferring data in an insecure manner | x | | | | x | | |
| Deliberate actions to breach data protection or network security rules | x | x | | | x | | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | x | x | | | x | | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | x | x | x | | x | | x |
| Using personal email / social networking / instant messaging / text messaging to carry out digital communications with learners | x | x | | | | | x |
| Actions which could compromise the staff member's professional standing | | | | | | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | x | x | | | | | x |
| Using proxy sites or other means to subvert the school's filtering system | x | x | | | | | x |
| Accidentally accessing offensive or pornographic material and failing to report the incident | x | | | | | | |
| Deliberately accessing or trying to access offensive or pornographic material | x | x | | | | | x |
| Breaching copyright or licensing regulations | x | | | | x | | |
| Continued infringements of the above, following previous warnings or sanctions | x | x | | | | | x |

**Acknowledgements**

WG 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 e-Safety Policy Template and of the 360 degree safe e-Safety Self Review Tool:

- Members of the SWGfL e-Safety Group
- Representatives of SW Local Authorities
- Representatives from a range of Welsh schools involved in consultation and pilot groups
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

**A1 Learner Acceptable Use of ICT Agreement – for learners in Reception, Year 1 and Year 2**

**This is how we stay safe when we use computers:**

I will ask a teacher or another adult from the school if I want to use the computers.

I will only use activities that a teacher or another adult from the school has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or another adult from the school if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (parent or carer) …….…….

Print name ……...

On behalf of (child's name) ……

Date …….

## A2 Learner Acceptable Use of ICT Agreement – for learners in Years 3 to 6

### School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Agreement is intended to ensure:**

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use;
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

### Acceptable Use 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.

**For my own personal safety:**

- I understand that the school will monitor my use of IT systems, devices and digital communications;
- I will keep my username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line;
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc );
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me;
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

**I understand that everyone has equal rights to use technology as a resource and:**

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission;
- 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 use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

**I will act as I expect others to act toward me:**

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will not take or distribute images of anyone without their permission.

**I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**

- I will not bring my own personal device(s) for use in school.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering and security systems in place to prevent access to such materials;
- I will immediately report any damage or faults involving equipment or software, however this may have happened;
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person or organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings;
- I will only use social media sites with permission and at the times that are allowed.

**When using the internet for research or recreation, I recognise that:**

- I should 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 try to download copies (including music and videos);
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school

and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information);

- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network and internet, detentions, suspensions, contact with parents and, in the event of illegal activities, the involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

**Learner Acceptable Use Agreement Form**

This form relates to the learner Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school);
- I use my own devices in the school (when allowed), for example, mobile phones, gaming devices, cameras etc;
- I use my own equipment out of school in a way that is related to me being a member of this school, for example, communicating with other members of the school, accessing school email, VLE, website etc.

| | |
|---|---|
| Name of Learner | |
| Class | |
| Signed | |
| Date | |

**Parent / Carer Countersignature**

| | |
|---|---|
| Name of Parent / Carer | |
| Signed | |
| Date | |

## A3 Acceptable Use of ICT Agreement – staff and volunteers

### School Policy

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 communications 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.

### 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 learners learning and will, in return, expect staff and volunteers to agree to be responsible users.

### 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 learners 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.

### 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 (eg 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;
- 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 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 and 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 (eg 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;
- I will only communicate with learners and parents / carers using official school systems. Any such communication will be professional in tone and manner;
- 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 my personal mobile device during contracted hours;
- 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 approved in advance by the Headteacher or e-Safety coordinator;
- 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 learner 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 a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

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 | |

**A4a Parent / Carer Acceptable Use of ICT Agreement – learners in Reception, Year 1 and Year 2**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that parents and carers are aware of the importance of e-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the Learner Acceptable Use Agreement is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

**Permission Form**

| | |
|---|---|
| Parent / Carer's Name | |
| Learner Name | |

As the parent / carer of the above learner, I give permission for my child to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, e-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

**P.T.O**

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

| | |
|---|---|
| Signed | |
| Date | |

**A4b Parent / Carer Acceptable Use of ICT Agreement – learners in Years 3 to 6**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that parents and carers are aware of the importance of e-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the Learner Acceptable Use Agreement is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

**Permission Form**

| | |
|---|---|
| Parent / Carers Name | |
| Learner Name | |

As the parent / carer of the above learner, I give permission for my child to have access to the internet and to ICT systems at school.

I know that my child has signed an Acceptable Use Agreement and has received, or will receive, e-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also

understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Signed

Date

**A5 Acceptable Use of ICT 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 | |

## A6 Use of Digital and Video Images

**Use of Digital and Video Images**

The use of digital and video images plays an important part in learning activities. Learners and members of staff may use digital devices to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. We will ensure that, when images are published, learners cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents or carers comment on any activities involving other learners in the digital or video images.

Permission can be withdrawn at any time by contacting the school office.

**Digital / Video Images Permission Form**

Learner's name ……

I give permission for my child's:

| | |
|---|---|
| Image to be used as part of school wall displays or class activities | Yes / No |
| Named work to be displayed around the school on wall displays | Yes / No |
| Image to be used in other learners' work books (for example, when taking part in a group activity) | Yes / No |
| Image and work to be stored on their Hwb account | Yes / No |
| Group image and group work to be stored on other learners' Hwb accounts | Yes / No |
| Image (not named) to be used on the school website | Yes / No |
| Image (not named) to be used in external media (for example, local newspaper press release) | Yes / No |
| Image to be included in the school's annual formal class or whole-school photographs | Yes / No |
| Image to be included in the school's annual formal individual photographs | Yes / No |
| I agree that if I take digital or video images at, or of, school events which include images of children other than my own, I will abide by the above guidelines in my use of these images | Yes / No |

Signed …….

Print name ……...

Date …….