Nant-y-Parc Primary School

E-Safety

2024-2025

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

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- Headteacher – Mrs. N. Davies
- e-Safety ICT Coordinator – Mr S. Tilley
- Staff – including teachers, support staff
- e-Safety Governor and E-Safety Team
- Parents and Carers
- School Council

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

Schedule for Development / Monitoring / Review

This e-safety policy was last approved by the Governing Body in June 24	
The implementation of this e-Safety policy will be monitored by the: HT, DHT and ICT e-Safety coordinator co-ordinator	
Monitoring will take place at regular intervals: Annually alongside e-Safety Team	
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: Annually Summer term	
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: April 2020	
Should serious e-Safety incidents take place, the following external persons/agencies should be informed: Helen West, LA Safeguarding Officer. Christopher Williams, LA Internet coordinator	

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of
  - students/pupils
  - parents/carers
  - staff

<u>E-Safety Team</u>

At Nant Y Parc Primary, we strive to ensure our pupils have the best experiences when using digital resources and ensuring our pupils are safe and confident individuals is vital in developing digital citizenship. At Nant Y Parc Primary, we have an e-Safety team that meets once a term to discuss internet safety and deliver training. Parents and governors who are members challenge the team to ensure we have a strong policy and digital learning experience.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals[1] and groups within the school:

Governors:

Governors are responsible for the approval of the 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 should take on the role of e-Safety Governor[2] to include:

- regular meetings with the e-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering/change control logs (where possible)
- reporting at Governors' meetings
- E-safety team meetings

Headteacher:

- The Headteacher has a duty of care to ensure the safety (including e-Safety) of members of the school community.

- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (Contact Intake and Assessment duty officer social services.

- The Headteacher is 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 Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Senior Management Team will receive regular monitoring reports from the e-Safety Co-ordinator

E-Safety Coordinator:

The e-Safety Coordinator (Mr Simon Tilley)

- leads the e-Safety Committee / Team.
- takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with the Local Authority / relevant body
- receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
- Meet regularly with the e-Safety *Governor* to discuss current issues, review incident logs and if possible, filter/change control logs.
- attends relevant meetings of *Governors*
- reports regularly to the Senior Leadership Team

Network Manager (Chris Williams. LA):

Our school has a managed ICT service provided by an outside contractor (LA), 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.

1.
2.

The Network Manager is responsible for ensuring:

- that the school's *technical* infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) the required e-Safety technical requirements as identified by the Local Authority and also the e-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the filtering policy is applied and updated regularly and its implementation is not the sole responsibility of any single person
- that they keep up to date with e-Safety technical information to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the network/internet / Virtual Learning Environment / remote access/email is regularly monitored so that any misuse / attempted misuse can be reported to the Headteacher e-Safety Coordinator for investigation
- that monitoring software/systems are implemented and updated as agreed in school   policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood, and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher and e-Safety Coordinator for investigation following the school's flowchart
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-Safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies about these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Safeguarding Designated Person (HT)

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 may choose to combine the roles of Safeguarding Officer and e-Safety Officer.

The Safeguarding Designated Person should be trained in e-Safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data[3]
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Team

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. Members of this group are currently Nicola Davies (Who meets during the summer term during Governor's meetings), Simon Tilley, Luke Smalley, A member of the Governing body, a parent and digital leaders. The group will also be responsible for regular reporting to the Governing Body.

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

- the production/review/monitoring of the school e-safety policy/documents.
- mapping and reviewing the e-Safety curricular provision — ensuring relevance, breadth and progression
- monitoring network/internet/incident logs where possible

- consulting stakeholders – including parents/carers and the students/pupils about the e-safety provision
- monitoring improvement actions identified through the use of the 360-degree safe Cymru self-review tool
- Testing new technologies and sharing good practice events

Pupils:

- are responsible for using the school's digital technology systems per the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and cyberbullying.
- should understand the importance of adopting good e-safety practices 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 in the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices appropriately. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practices and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and online student/pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems/websites / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. Currently would be an afterschool club and Youth Club

Blended Learning / Covid- 19

Due to the current climate Blended learning has become a large part of teaching and learning. To ensure the safety of our staff and pupils we have created a Home Learning / Blended Learning Agreement / Policy.

Home Learning Agreement

At Nant y Parc we feel very passionate about working closely with our parents and community. This distance learning home-school agreement has been devised to ensure that parents and pupils have a consistent and reinforced message in the expectations of their learning at home.

Pupil Expectations:-

- Ensure you bring in your distance learning bag and both books on your first day of returning to school. Your 'first day' means the day you return following home learning.
- Access your virtual classroom via the school website, Google Classroom or Seesaw App.
- Ensure you know how to navigate SeeSaw (N-Y4) or Google Drive/Google Classroom (Y5-Y6) to access the work set to you.
- Engage with the videos presented by your class teacher. These will support your learning. See the video column for lessons with accompanying videos.
- When completing tasks, present them in your linking learning books or via an online platform where applicable.
- Take care with presentation in your linking learning books, these books will be marked.
- If tasks are required to be submitted digitally, you will be told about this and shown how to do this.
- Try to keep a positive attitude to your learning. If challenged, be resilient and do not give up trying.
- Ensure that you take adequate rest and a break from school tasks during the day.
- Ask your parents/carer for help or email your teacher/access live videos and drop-in sessions
- Follow the Home Learning Rules provided by your teacher during Live streaming sessions (See Live streaming)

Parent / Guardian Expectations

- Ensure your child brings in their linking learning book the first day they return to school following a home learning period.

- Engage in parent drop-in sessions if you feel this is required for the set learning tasks.
- Don't be afraid to seek guidance where necessary by contacting the school or your child's class teacher.
- Support your child with their home learning and encourage them to engage in the tasks set.
- Recognise the importance of tasks that seek to develop important literacy and numeracy skills.
- Provide your child with praise - we know how important this can be with this new way of learning.
- Ensure that your child takes adequate rest and breaks from learning activities/tasks.
- Refer to the distance learning policy if required.
- If you require additional help or support or have any general queries regarding Home learning you can contact the info@nantyparc.org email. You can also refer to the school's Twitter (now formerly known as X) @Nantyparcschool and the school's website www.nantyparcprimaryschool.co.uk

Teacher Expectations

- Provide resources for all learning activities.
- Provide clear guidance on task expectations.
- Ensure pupils are given guidance (during their contact time in school) on how to use Google Drive/Google Classroom/SeeSaw and the virtual classroom.
- Ensure that there are "How to" guides will be available as videos on the school website for parents to access online learning platforms.
- Mark submitted work by the given deadline.
- Monitor pupil participation/engagement and report any concerns to SLT.
- Award house points for efforts in learning and behaviour.
- Respond to SeeSaw or Google Classroom posts/emails within school hours (08:00 - 17:00)
- Be available online at an allocated time to answer questions specific to year-group learning tasks.
- Topics will be aligned within phases to allow for siblings from different year groups to work together and support each other.
- Topics will be differentiated for each year group

Live Streaming

- The time and date of live streaming will be shared in advance by the class teacher with parents.
- Pupils to ensure devices are ready and charged for the sessions.
- Staff to introduce rules and aims at the start of each live session
- Appropriate behaviour is always expected. I will be responsible for my behaviour and actions when using technology, this includes the resources I access and the language I use.
- Pupils / Staff will wear appropriate clothing or a school jumper/t-shirt.
- Pupils to choose whether to turn the camera on / off. An appropriate image for the profile must be set.
- Pupils will have the choice to turn Audio on / off.
- Pupils/staff should access live streaming in a suitable room where there is strong internet access — avoid busy places, and interruptions from other family members or pets.
- Pupils/staff should avoid using personal rooms — No bedrooms and consider the background.
- Pupils to enter the live session with the microphone on mute.
- To protect staff and pupils, live streaming will be recorded and saved when live streaming ends.
- Live streaming will be for pupil-teacher communication only. Parents are to contact the school/email the class teacher with any queries.
- All pupils to leave live streaming by clicking the 'Leave conversation' text. I will only take part in 'live' streaming if an adult knows that I am doing it.
- I will not reveal my passwords to anyone.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher or my parent.
- I will not share resources or videos created by my teachers with anyone who is not a pupil or member of staff at Nant y Parc Primary School, and I will not record or take photos of my classmates or teachers during a face-to-face session.
- I will not share any school content on social media platforms.

- I understand that when using Live streaming and other applications provided by the school my use can be monitored and logged and can be made available to my teachers.

Safeguarding

In the event of a school closure, pupils, parents and teachers are reminded that the school's Child Protection and Safeguarding Policy still applies to all interactions between pupils and teachers. In that policy, there are specifically prohibited behaviours and reporting obligations to which teachers must adhere, whether they are at home, in the community or at school.

Signed _____ (Parent / Guardian)

Date   _____

Signed _____ (Pupil)

Date   _____

Signed _____ (Teacher)

Date   _____

Policy Statements

Education — young people

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of pupils in e-Safety is therefore an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-Safety curriculum should be provided as part of ICT / PSE / Digital Literacy lessons or other lessons and should be regularly revisited (We have adopted the WG's SOW)
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and activities
- Pupils 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils 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 LA can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Education – parents/carers

Many parents and carers have only a limited understanding of e-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 will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE, Twitter
- Parents / Carers evenings/sessions
- High-profile events/campaigns e.g. Safer Internet Day / Nant E Parc
- Reference to the relevant websites/publications e.g. https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers and opportunities to attend training with the E-Safety team.

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in the use of new digital technologies, digital literacy and e-Safety
- e-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school VLE / website will provide e-safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports / voluntary groups to enhance their e-Safety provision (possibly supporting the group in the use of Online Compass, an online-Safety self-review tool – www.onlinecompass.org.uk)

Education & Training – Staff / Volunteers

All staff must 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.
- 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 (e.g. from Consortium/ LA / 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/team meetings / INSET days.
- The e-Safety Coordinator will provide advice/guidance/training to individuals as required.

Training – Governors

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

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

Technical – infrastructure/equipment, filtering and monitoring

Our 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 / Acceptable Use Agreements.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:
- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority / other relevant body policy and guidance)
- There will be regular reviews and audits of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2) will be provided with a username and secure password by Mr Tilley who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password (We use group or class log-on and passwords for KS1 and below, but need to be aware of the associated risks – see appendix)
- The "master/administrator" passwords for the school ICT system, used by the Network Manager (or another person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- Simon Tilley is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored
- The school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils / etc)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils 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 pupils 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 images on the internet e.g. on social networking sites.
- Following guidance from the Information Commissioner's Office, parents/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/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution, and publication of those images. Those 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 / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' 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 pupils are published on the school website/ Google/Hwb
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection / GDPR

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 under the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Our school has ensured 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 the data held is accurate, and 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 following the "Conditions for Processing". (see Privacy Notice section in the appendix)
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the Data Protection Act (DPA)**
- **ST has delivered GDPR Training to all staff and more information is available on the website**
- Responsible persons are appointed/identified - Senior Information Risk Officers (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" 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 policy (below) once it has been transferred or its use is complete

(The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted — some organisations do not allow storage of personal data on removable devices.)

The Personal Data Handling Policy Template in Appendix B2 provides more detailed guidance on the school's responsibilities and on good practice.

Communications

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree on how they intend to implement and use these technologies e.g. few schools allow students/pupils 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 students/pupils. The table has been left blank for the school 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 currently considers the benefits of using these technologies for education to outweigh their risks/disadvantages:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons	✓							✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones/cameras			✓					✓
Use of other mobile devices e.g. tablets, gaming devices	✓						✓	
Use of personal email addresses in school, or on the school network			✓					✓
Use of school email for personal emails			✓				✓	
Use of messaging apps	✓							✓
Use of social media	✓						✓	
Use of blogs	✓					✓		

The school 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 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 pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report to the nominated person – under 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 pupils or parents/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.
- Whole class/group email addresses may be used at KSI, while students/pupils at KS2 and above will be provided with individual school email addresses for educational use.
- pupils should be taught about e-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 website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in the use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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

The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school by 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 pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the social media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable/inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would be banned from school and all other technical systems. Other activities eg 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:

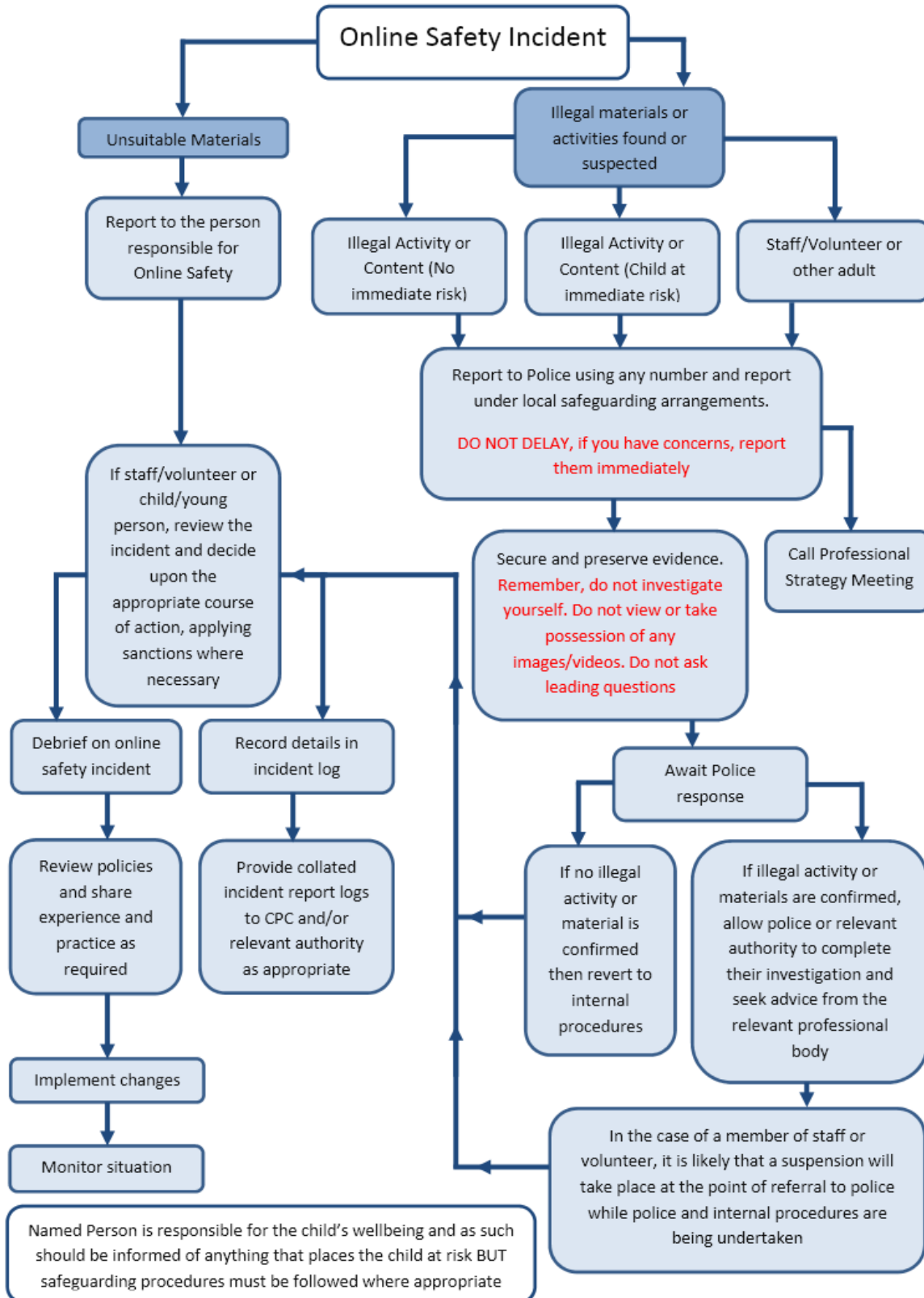| User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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 the 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 (e.g. 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 hinder others in their use of the internet)					X	
On-line gaming (Educational)						
On-line gaming (non-educational)						
Online gambling						
Online shopping/commerce						
File sharing						
Use of social media						
Use of messaging apps						
Use of video broadcasting e.g. YouTube						

(The school should agree on its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for schools to decide their responses)

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 website 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

- Report to the person responsible for Online Safety
- If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
  - Debrief on online safety incident
    - Review policies and share experience and practice as required
      - Implement changes
        - Monitor situation
  - Record details in incident log
    - Provide collated incident report logs to CPC and/or relevant authority as appropriate

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

Illegal materials or activities found or suspected

- 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

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

Await Police response

- 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

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

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off-site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff 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 the 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.**

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

School Actions

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

School E-Safety Team Incident

To ensure our school is digitally safe we need to ensure the procedure is clear and consistent to ensure the safety of our pupils and staff. Here is an outline of who you can talk to and what to do if there is an E-Safety incident.

- Inappropriate use of technology
- Cyberbullying
- Using technology that is not appropriate
- Damaging or attempting to break / damage/ alter digital technology

If there is an E-Safety incident, you will need to speak to the appropriate member of staff. If you believe the issue to be a safeguarding issue, then you must follow the safeguarding procedure. For other digital incidents, you would need to report to a senior member of the E-Safety Team.

Mr. S. Tilley & Mr. L. Smalley are all members of the e-Safety Team.

Pupils

Incidents:	Refer to class teacher/tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	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 e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/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						
Unauthorised use of social media/messaging apps / personal email			x						
Unauthorised downloading or uploading of files	x								
Allowing others to access the school network by sharing usernames and passwords			x						
Attempting to access or accessing the school network, using another student's / pupil's account			x			x			
Attempting to access or accessing the school network, using the account of a member of staff						x			x
Corrupting or destroying the data of other users						x			x
Sending an email, text or message that is regarded as offensive, harassing or of a bullying nature						x			x
Continued infringements of the above, following previous warnings or sanctions						x			x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system						x	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

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act					X		X	

Incidents:	Refer to the line manager	Refer to Head teacher Principal	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	x					
Unauthorised downloading or uploading of files		x	x					
Allowing others to access the school network by sharing usernames and passwords or attempting to access or accessing the school network, using another person's account			x					
Careless use of personal data e.g. holding or transferring data in an insecure manner			x					
Deliberate actions to breach data protection or network security rules			x					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software			x				x	
Sending an email, text or message that is regarded as offensive, harassing or of a bullying nature			x					x
Using personal email / social networking / instant messaging/text messaging to carry out digital communications with students/pupils			x					x
Actions which could compromise the staff member's professional standing			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		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

Breaching copyright or licensing regulations			x					
Continued infringements of the above, following previous warnings or sanctions			x					x

Appendices – Section A - Acceptable Use Agreement

- A1 Pupil Acceptable Use Agreement FP
- A2 Pupil Acceptable Use Agreement KS2
- A3 Staff and Volunteers Acceptable Use Agreement Template

Appendices – Section B – Specific Policies

- B1 School Technical Security Policy template   xx
- B2 School Personal Data Policy template   xx
- B3 School Bring Your Own Devices (BYOD) Template Policy   xx
                                                                                                              xx

Appendices – Section C – Support documents and links

- C1 Responding to incidents of misuse – flowchart   xx
- C2 Record of reviewing sites (for internet misuse)   xx
- C3 School Reporting Log template   xx
- C4 School Training Needs Audit template   xx
- C5 Summary of Legislation   xx
- C6 Office 365 – further details   xx
- C7 Links to other organisations and documents   xx
- C8 Glossary of terms   xx

Pupil Acceptable Use Policy Agreement Template – for younger pupils (PS1 & PS2)

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 (child):…………………………………………………
(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children, the signature of a parent/carer should be sufficient)

Signed (parent): …………………………………………………..

Primary schools using this acceptable use agreement for younger children may also wish to use (or adapt for use) the Parent / Carer Acceptable Use Agreement (the template can be found later in these templates) as this provides additional permission forms (including the digital and video images permission form).

Pupil Acceptable Use Agreement – for older pupils

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 *students/pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users.

Acceptable Use Agreement

I understand that I must responsibly use school ICT systems, to ensure that there is no risk to my safety or the safety and security of the ICT systems and other users.

For my 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 someone may steal it.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people offline that I have communicated with online, 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 online.

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 online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube) unless I have permission from 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 only use my device(s) in school if I have permission. I understand that, if I do use my device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- 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 programs 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 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/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 not use social media sites

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 in 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/internet, detentions, suspensions, contact with parents and in the event of illegal activities 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.

Pupil Acceptable Use Agreement Form

This form relates to the *student/pupil* 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) e.g. mobile phones, gaming devices, cameras etc
- I use my equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil	
Group / Class	
Signed	
Date	

Parent / Carer Countersignature (optional)

Note: It is for schools to decide whether or not they require parents/carers to sign the Parent / Carer Acceptable Use Agreement (see template later in this document). This includes several other permission forms (including digital and video images / biometric permission/cloud computing permission).

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 always have an entitlement to safe internet access.

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, and to enhance learning opportunities for *students/pupils* and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

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 the use of school ICT systems (e.g. laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper-based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where 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 professionally communicate with others, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and following the school's policy on the use of digital / video images. I will not use my equipment to record these images unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school following the school's policies. (Schools should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. (Schools should amend this section to take account of their policy on communications with students/pupils and parents/carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any online 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 were using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will ensure that my data is regularly backed up, following relevant school policies.
- I will not try to upload, download or access any illegal materials (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings unless this is allowed in school policies. (schools/academies should amend this section in the light of their policies on installing programmes / altering settings)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper-based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.

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

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

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

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

A4 Parent / Carer Acceptable Use Agreement Template

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 regarding their online behaviour.

The school will try to ensure that *students/pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Agreement is attached to this permission form so that parents/carers will be aware of the school's 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 Name		Pupil Name	

As the parent/carer of the above *pupils*, I permit my son/daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)
I know that my son/daughter 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.

Or: (KS1)
I understand that the school has discussed the Acceptable Use Agreement with my son/daughter 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.

I understand that my son's / daughter'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

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras/iPads 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,

The school will comply with the Data Protection Act and request parents'/carers' permission before taking images of members of the school. We will also ensure that when images are published the young people cannot be identified using their names.

Following guidance from the Information Commissioner's Office, parents/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/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital / video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Digital / Video Images Permission Form

Parent / Carer Name

Student / Pupil Name

As the parent/carer of the above *student/pupil*, I agree to the school taking and using digital / video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

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 these guidelines in my use of these images.

Yes / No

Signed

Date

Use of Biometric Systems

The school uses biometric systems for the recognition of individual children in the following: Library.
Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them so nothing can be lost, such as a swipe card.

The school has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints are stored, and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents/carers are asked for permission for these biometric technologies to be used by their child:

Parent / Carer Name

Student / Pupil Name

As the parent/carer of the above *student/pupil*, I agree to the school using biometric recognition systems, as described above. I understand that the images cannot be used to create a whole fingerprint/palm print of my child and that these images will not be shared with anyone outside the school.

Yes / No

Signed

Date

B2 School Personal Data Handling Policy Template

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner Office. for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

Policy Statements

The school 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 the data held is accurate, and up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained following the "Privacy Notice" and lawfully processed following the "Conditions for Processing". (See Privacy Notice section below)

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils/students*, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Responsibilities

The school's Senior Information Risk Officer (SIRO) is This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) *for the various types of* data being held (e.g. pupil/student information/staff information/assessment data etc). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose.
- how information has been amended or added to over time, and
- who has access to protected data and why?

Everyone in the school has the responsibility of handling protected or sensitive data safely and securely.

Governors are required to comply fully with this policy if they have access to personal data when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner

Information to Parents / Carers – the "Privacy Notice"

To comply with the fair processing requirements of the DPA, the school will inform parents/carers of all pupils/students of the data they collect, process and hold on the pupils/students, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom it

may be passed. This privacy notice will be passed to parents/carers through. Parents/carers of young people who are new to the school will be provided with the privacy notice.

.

Training & awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through Induction training for new staff

- Staff meetings/briefings / Inset
- Day-to-day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost-effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	

PROTECT	1 or 2	Will apply in schools
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The terms 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements in a report or data view increases the impact of a breach. A breach that puts students/pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than the damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly User passwords must never be shared.

Personal data may only be accessed on machines that are securely password-protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto-lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media Private equipment (e.g. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB 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 (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policies and procedures for the automatic backing up, accessing, and restoring all data held on school systems, including off-site backups.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Office365) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud-based data service providers to protect the data.: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx)

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper-based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off-site.

The school recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have several rights in connection with their personal data, the main one being the right of access. Procedures are in place (insert details here) to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out-of-school

The school recognises that personal data may be accessed by users out of school or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted, and password protected and is transported securely for storage in a secure
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, following government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, with respect to electronically held personal data, will be logged and these logs will be monitored by responsible individuals. (insert name or title). The audit logs will be kept providing evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes: (schools should determine their own reporting policy, in line with that of their LA (if relevant), and add details here)

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based on the local incident handling policy and communication plan.

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupil's work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portals, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil/student academic, social, and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically, schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil/student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about school closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendices: Additional issues/documents related to Personal Data Handling in Schools:

Use of Biometric Information

The Protection of Freedoms Act 2012, includes measures that will affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools and colleges under 18, must obtain the written consent of a parent before they take and process their child's biometric data.
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 1998.
- They must provide alternative means for accessing services where a parent or pupil has refused consent.

Schools will no longer be able to use pupils' biometric data without parental consent. The advice came into effect in September 2013. Schools may wish to consider these changes when reviewing their Personal Data Handling Template. Schools may wish to incorporate the parental permission procedures into existing parental forms (e.g. AUP / Digital & Video Images permission form).

Use of Cloud Services

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

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

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

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

Freedom of Information

FOI may require anything you write in an official capacity to be potentially made public. This might mean you need to consider how long content is stored and the ease with which it can be recovered from a cloud archive.

Cloud services very often are not designed for the long-term storage of content, particularly transient communications with high volumes like email. Schools should consider how to secure and back up to a local system what could be sensitive or important data.

A summary of good practice in dealing with requests can be found [here](#)

Data Protection Act

Schools, like any other organisation, are subject to the Data Protection Act (DPA) and its eight basic principles. The DPA refers to 'personal data' – this can be described generally as information which identifies an individual and is personal to an individual.

The DPA contains eight 'Data Protection Principles' which specify that personal data must be:

- Processed fairly and lawfully
- Obtained for specified and lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept any longer than necessary
- Processed following the 'data subject's' (the individual's) rights
- Securely kept
- Not transferred to any other country without adequate protection

It's also worth considering that whilst not all data is 'personal', the information that is, has varying levels of sensitivity based on the impact were it to be compromised.

The Information Commissioners Office has produced a report aimed at helping schools meet their data protection obligations; you can read the report detailing data protection advice for schools here and a simple summary of the report here.

Safeguarding

There are also safeguarding obligations for the use of technology in schools that include (possibly in partnership with your service provider):

- Effectively monitoring the use of systems to detect potential and actual safeguarding issues
- Monitoring, alerting and responding to illegal activity
- Providing consistent safeguarding provision both within and beyond school if devices/services leave the site

Criminal Activity

Schools have an immediate obligation to report illegal or criminal activity to the Police. A detailed summary of legislation that pertains to safeguarding and schools can be found elsewhere in this documentation.

Other services e.g. Facebook, Twitter, etc are useful cloud tools in and beyond the classroom but it is important to be aware of age restrictions here too. US Law requires any company operating within the US to comply with the Children's Online Privacy Protection Act (COPPA) which legislates against companies who store, process and manage information on children aged 13 and under and the active or targeted marketing to that age group.

Where is the cloud?

Most education systems have to make use of personal information to function. The DPA (Principle 8) states that personal data must not be transferred to any other country without adequate protection in situ. Data protection requirements vary widely across the globe. Countries in the EU approach privacy protection differently from those outside and are more stringent in the details and responsibilities of data users than perhaps the US. Microsoft Office 365 is held in data centres in Amsterdam and Dublin.

Security concerns

Can anyone access data in the cloud centre where it sits? Data centres are required to have stringent physical interventions in place against data being compromised from internal or external access. There are sophisticated security mechanisms in place to prevent external hacking of data. Whilst this cannot always be guaranteed to be 100% safe, this sophistication is often beyond the local capability of a single school and so can be regarded as a reasonable duty of care.

Access to data through devices is much more likely given that devices are going to and from school in bags, on buses, or left lying around at home or school so security now becomes much more of an issue at a user level than it ever has before. If a device goes missing or breaks, the big advantage of cloud systems is that, apart from simple local settings, content is in the cloud, so data is not 'lost' in the same way as if your laptop was stolen or suffered a hard drive failure. Cloud services can offer device management systems that can lock or locate a device if missing.

Passwords and authentication are critical at any point in securing access to data but are especially so with data in the cloud. Some points to consider are:

- Are passwords strong?
- Do users know what a strong password looks like?
- Do you insist on rolling user passwords regularly? Every 60 days? Many businesses do as good practice.
- Are users educated in good password practice? Is this backed up with a clear and reliable password policy?

If you need a template, then one can be found as part of this policy suite.

It's also important to ensure there is a clear and reliable culture around reporting issues such as compromise, loss or unethical practice. This doesn't happen on its own and needs to be taught. Again, the common sense, everyday good practice around logging out of systems when finished, having a management plan in place if something goes wrong, and having reporting mechanisms in place also applies to using cloud technologies. For example, Southwest Grid for Learning has produced a free Digital Literacy and Citizenship Curriculum for PS1 TO PS3 which has a variety of strands one of which focuses on Privacy and Security. Pupils and students learn strategies for managing their online information and keeping it secure from online risks such as identity thieves and phishing. They learn how to create strong passwords, how to avoid scams and schemes, and how to analyse privacy policies. The version of this resource for Wales is available via HWB (November 2014).

Monitoring users

Local networks based on site have the advantage of being relatively easy to filter and monitor for inappropriate or illegal use and many schools will already have these systems in place. Filtering can be provided as part of a school's internet provision, particularly if they have that service delivered through the local/unitary authority. A school may choose to provide its own through a variety of commercial solutions.

However, when services move into a wider cloud-based environment hosted by an external partner it becomes more difficult to know what users are storing or accessing, particularly if their connectivity away from the school is a domestic one.

With all of those separate user folders and portfolios with their separate passwords and widely varying content, how can you be sure they are not being used to store inappropriate materials? Illegal materials? The school provides the tools e.g. Office 365 and there is therefore an expectation that the school should ensure that users are operating in a space that is safe as can be created.

Microsoft states in their user agreements that they reserve the right to actively search stored files.

This means that the school also needs to be clear about what the expectations are around illegal and inappropriate content and how it intends to ensure those expectations are met. These might include:

- Clear and effective agreement through an Acceptable Use Policy or computer splash screen with an "agree" button
- Positive statements around the use of technology dotted around areas where that technology might be used (particularly effective are student-designed posters)
- Active education in raising awareness of what illegal or inappropriate mean
- Staff development in recognising and escalating reports of illegal content
- Reminders that Cloud Service Providers can and do scan content stored on their servers and that an archive exists
- Establish regular spot checks on mobile devices and advertise the fact that these will be carried out on school devices and removable media
- Establish and communicate that One Drive provided as part of a school cloud solution will be subject to random spot checks by resetting passwords back to default to allow auditing or set the expectation that users should share their online folders with their teacher. The system has been provided for educational use so there should not be anything in there that isn't related to learning.

Managing accounts and users

Dealing with one tablet or smartphone on your own account is empowering; you can make choices about how you set it up, the apps you want; the subscriptions you choose and how many photos or documents to store on it. Setting up tens of devices with potentially hundreds of users has a whole different set of considerations:

- The distribution and timetabling of school-owned devices (particularly those that go home?)
- Can users store content locally on the tablet e.g. photos?
- Can school network and connectivity sustain the use of many devices?
- Is there one standard profile for everyone or can each user customise?
- How are those profiles managed or swapped?
- Are personal devices allowed to be commissioned to the school system (BYOD)?

A Mobile Device Management layer can be critical in establishing access rights to these technologies. You may need to consult with your service provider to investigate what options are available to you.

If things go wrong

Like any other safeguarding issue, there must be clear and rigorous incident management practices that are consistent with other safeguarding policies.

- Clear and well-communicated policy
- Effective routines for securing and recording evidence
- Established reporting routes that are well-communicated, respected and agreed by all
- Clearly communicated sanctions that have been agreed and shared with all users
- Audit trails that are used to shape interventions and inform future practice

What policies and procedures should be put in place for individual users of cloud-based services?

The school is ultimately responsible for the contract with the provider of the system.

Appendix C6 provides a useful summary of issues around Office 365 written with the support of Microsoft:

The document focuses on Office 365 but poses important considerations if a school is considering services from another provider.

Privacy and Electronic Communications

Schools should be aware that the Privacy and Electronic Communications Regulations have changed and that they are subject to these changes in the operation of their websites.

Freedom of Information Act

All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy, the school should:

- Delegate to the Headteacher / Principal day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy.
- Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need.
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body.
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually.
- Ensure that a well-managed records management and information system exists to comply with requests.
- Ensure a record of refusals and reasons for refusals is kept, allowing the Academy Trust to review its access policy on an annual basis.

Model Publication Scheme

The Information Commissioners Office provides schools with a model publication scheme which they should complete. This was revised in 2009, so any school with a scheme published before then should review this as a matter of urgency. The school's publication scheme should be reviewed annually.

Guidance on the model publication scheme can be found at:

The Schools Model Publication Scheme Template is available from:

Further Guidance

ICO guidance can be found at the following link - including a pdf version - updated in September 2012:
http://www.ico.gov.uk/for_organisations/freedom_of_information/guide.aspx

B3 School Bring Your Own Devices (BYOD) Policy

Devices are brought into the school entirely at the risk of the owner and the decision to bring the device into the school lies with the user and their parents/carers as does the liability for any loss or damage resulting from the use of the device in school.

The school accepts no responsibility or liability in respect of lost, stolen, or damaged devices while at school or on activities organised or undertaken by the school.

The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network.

The school recommends that the devices be made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Passcodes or PINs should be set on personal devices to aid security.

The school is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

BYOD access will not be permitted without authorisation through the return of the Acceptable Use Agreement permission slip which has been countersigned by the parents/carers of the student.

Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements
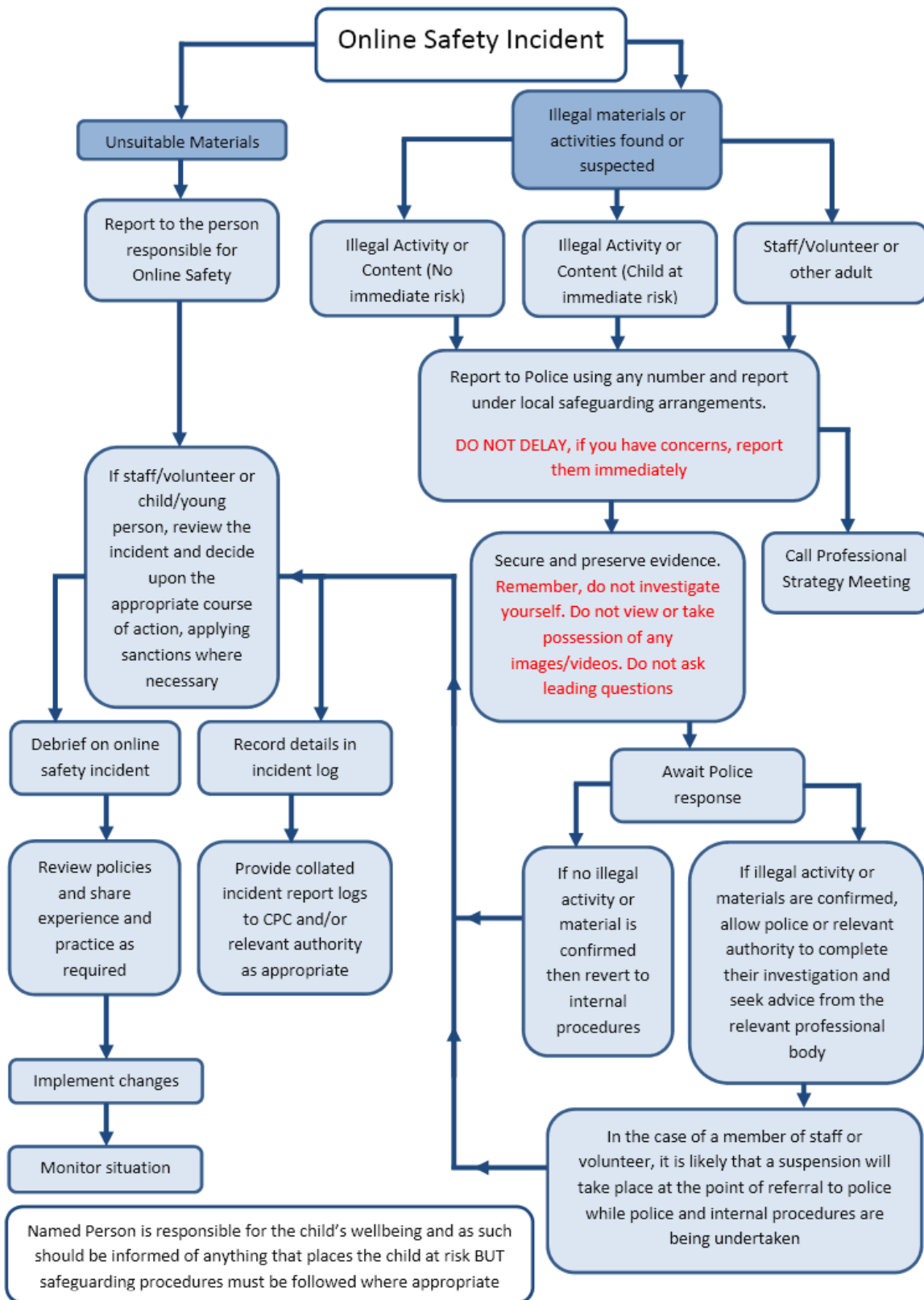Users are responsible for keeping their devices up to date through software, security and app updates
Users are responsible for charging their own devices and for protecting and looking after their devices while in school many issues discussed by this group could be of a sensitive or confidential nature.
2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave

the meeting with steps being made by the other members to allow for these sensitivities.

CI Responding to incidents of misuse – flow chart

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

C2 Record of reviewing devices/internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of the second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for websites)

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log Group	Signature									
	Incident Reported by									
	Action taken	By whom?								
		What?								
	Incident									
	Time									

	Date								

C4 Training Needs Audit

	Review date								
Training Needs Audit Log Group .... Date	Cost								
	To be met by:								
	Identified training need								
	Relevant training in last 12 months								

	Position								
	Name								

C5 Summary of Legislation

Schools should be aware of the legislative framework under which this e-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e-safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed by the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow several set procedures.

Communications Act 2003

Sending using the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message using or persistently making use of the Internet to cause annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, grossly offensive, or threatening letter, electronic communication, or another article to another person. It is also an offence to send information which is false and known or believed to be false by the sender.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Where the system controller has given express consent monitoring or keeping a record of any form of electronic communications is permitted, to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible to:
- Ascertain whether the communication is business or personal;
- Protect or support helpline staff.

Trade Marks Act 1994

This protects Registered Trademarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all or a substantial part of a copyrighted work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Criminal Justice & Public Order Act 1994 / Public Order Act 1986

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006 / Public Order Act 1986

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing, or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality, or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence is liable to imprisonment for a term of not more than 10 years, or a fine or both.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world to commit a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, and connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing, or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience, and religion
- Freedom of expression

- Freedom of assembly
- Prohibition of discrimination
- The right to education
- The right not to be subjected to inhuman or degrading treatment or punishment

The school is obliged to respect these rights and freedoms but should balance them against those rights, duties, and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

C6 Office 365 — further information

Where is the data stored?

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

How often is the data backed up?

The idea of "backup" is very different with Office365 than with traditional locally hosted services. We use a network of globally redundant data centres and replicate data on multiple servers across the two data centres. At any one time, we keep 3 copies of the school's data across the two data centres mentioned (Dublin & Amsterdam).

Does the email service provider have a clear process for recovering data?

Yes. Users themselves can recover data for 30 days after deleting an item. Administrators then have a further 30 days once the item is deleted from the deleted items folder. There are also additional paid-for archiving services available with Office365, but with a 25GB inbox per person, the pressure on users to archive email is not as great compared to existing email systems.

How does the email provider protect your privacy?

3 key things: No advertising, no "mingling" of Office 365 data with our consumer services (such as Hotmail) and full data portability, in case you ever want to leave the service.

Who owns the data that you store on the email platform?

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

Who has access to the data?

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

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

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

Is personal information shared with anyone else?

No personal information is shared.

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

No. There is no advertising in Office365.

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

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

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

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

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

How reliable is the email service?

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

What level of support is offered as part of the service?

Microsoft offer schools direct telephone support 24/7 for IT administrators and there is also a large range of online help services, which you can read about here. We recommend that schools use a Microsoft partner or support organisation with industry-specific expertise in cloud services for schools.

Additional Resources

There is a wealth of information about Office365 in the Office365 Trust Centre. You can also read articles about Office365, get deployment resources and contact Microsoft Cloud experts directly on their UK Schools Cloud Blog.

C7 Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

UK Safer Internet Centre

- Safer Internet Centre
- South West Grid for Learning
- Childnet
- Professionals Online-Safety Helpline
- Internet Watch Foundation

CEOP

- http://ceop.police.uk/
- ThinkUKnow

Others

- INSAFE – http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- UK Council for Child Internet Safety (UKCCIS) – www.education.gov.uk/ukccis
- Netsmartz – http://www.netsmartz.org/index.aspx

Support for Schools

- Specialist help and support   – SWGfL BOOST

Cyberbullying

- Scottish Anti-Bullying Service, Respectme – http://www.respectme.org.uk/
- Scottish Government – Better relationships, better learning, better behaviour
- Welsh Government – Respecting Others
- Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org – http://www.cyberbullying.org/

Social Networking

- Digizen – Social Networking
- SWGfl – Facebook – Managing risk for staff and volunteers working with children and young people
- Connectsafely Parents Guide to Facebook
- Facebook Guide for Educators

Curriculum

- SWGfL Digital Literacy & Citizenship curriculum
- Alberta, Canada - digital citizenship policy development guide.pdf
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources
- Somerset - e-Sense materials for schools

Mobile Devices / BYOD

- Cloudlearn Report Effective practice for schools moving to end locking and blocking
- NEN - Guidance Note - BYOD

Data Protection

- Information Commissioners Office:

  - ➤ Your rights to your information – Resources for Schools - ICO
  - ➤ ICO pages for young people
  - ➤ Guide to Data Protection Act - Information Commissioners Office
  - ➤ Guide to the Freedom of Information Act - Information Commissioners Office
  - ➤ ICO guidance on the Freedom of Information Model Publication Scheme
  - ➤ ICO Freedom of Information Model Publication Scheme Template for schools (England)
  - ➤ ICO - Guidance we gave to schools - September 2012 (England)
  - ➤ ICO Guidance on Bring Your Own Device
  - ➤ ICO Guidance on Cloud Hosted Services
  - ➤ Information Commissioners Office good practice note on taking photos in schools
  - ➤ ICO Guidance Data Protection Practical Guide to IT Security
  - ➤ ICO – Think Privacy Toolkit
  - ➤ ICO – Personal Information Online – Code of Practice
  - ➤ ICO – Access Aware Toolkit
  - ➤ ICO Subject Access Code of Practice
  - ➤ ICO – Guidance on Data Security Breach Management

- SWGfL - Guidance for Schools on Cloud Hosted Services
- LGfL - Data Handling Compliance Check List
- Somerset - Flowchart on Storage of Personal Data
- NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

- DfE - Safer Working Practice for Adults who Work with Children and Young People
- Kent - Safer Practice with Technology
- Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online-Safety Helpline

Infrastructure / Technical Support

- Somerset - Questions for Technical Support
- NEN - Guidance Note - esecurity SWGfl / Common Sense Media Digital Literacy & Citizenship Curriculum

Working with parents and carers

- SWGfl BOOST Presentations - parents presentation
- Connect Safely - a Parents Guide to Facebook
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers

- [DirectGov - Internet Safety for parents](#)
- [Get Safe Online - resources for parents](#)
- [Teach Today - resources for parents workshops / education](#)
- [The Digital Universe of Your Children - animated videos for parents (Insafe)](#)
- [Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)
- [Insafe - A guide for parents - education and the new media](#)
- [The Cybersmile Foundation (cyberbullying) - advice for parents](#)

Research

- [EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)
- [Futurelab - "Digital participation - its not chalk and talk any more!"](#)

C8 Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young People Services (in Local Authorities)
FOSI	Family Online-Safety Institute
EA	Education Authority
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In-Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting.
WAP	Wireless Application Protocol