



Global Learning Programme Wales
Lead School



Ysgol Arweiniol
Rhaglen Dysgu Byd-Eang Cymru



Johnstown Primary School Ysgol Gynradd Tre Ioan



E-Safety Policy



A Sports Council for Wales Initiative
Menter gan Gyngor Chwaraeon Cymru



Contents

Introduction

School e-Safety Template Policy

Development, monitoring and review of the Policy

Schedule for development, monitoring and review

Roles and Responsibilities

- Governors
- Headteacher / Principal and Senior Leaders
- e-Safety Co-ordinator / Officer
- Network Manager / Technical Staff
- Teaching and Support Staff
- Safeguarding Designated Person / Officer
- e-Safety Committee
- Students / Pupils
- Parents / Carers
- Community Users

Policy Statements

- Education – Students / Pupils
- Education – Parents / Carers
- Education – The Wider Community
- Education and training – Staff / Volunteers
- Training – Governors
- Technical – infrastructure / equipment, filtering and monitoring
- Use of digital and video images
- Data protection
- Password Security
- Use of Cloud Services via HWB
- Communications
- Social Media - Protecting Professional Identity
- User Actions - unsuitable / inappropriate activities
- Responding to incidents of misuse

Appendices

- Staff - Communications Code of conduct (younger children)
- Pupil - Acceptable Use Agreement for Hwb (FP Learners)
- Pupil - Acceptable Use Agreement for Hwb (KS2 Learners)
- Staff - Acceptable Use Agreement for Hwb
- Parent - Acceptable Use Agreement Letter for Hwb
- Parent - Acceptable Use Agreement Letter for Digital Learning
- Pupil – e-Safety posters (FP Learners)
- Pupil – e-Safety posters (KS2 Learners)

- Staff – Training Needs Audit template
- Summary of Legislation
- Links to other organisations and documents

Introduction

The e-Safety Policy

Johnstown Primary School's e-Safety Policy is intended to help school leaders consider all current and relevant issues related to e-Safety in a whole school context, often linking these considerations with other relevant policies, such as the Safeguarding, Behaviour and Anti-Bullying policies.

The policy is designed to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely. This serves to address the wider duty of care to which all who work in the school are bound. The policy serves to ensure that all designated stakeholders uphold their statutory obligations so that children and young people are safe and protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

These template policies suggest policy statements which, in the view of Welsh Government, would be essential in any school e-Safety Policy, based on good practice. In addition there are a range of alternative statements that schools should consider and choose those that are most suitable, given their particular circumstances.

Johnstown Primary School's e-Safety policy has been tailored to the needs of our school, and an important part of this process has been the discussion and consultation which has taken place during the review of this most current policy. This helps to ensure that the e-safety policy is owned and accepted by the whole school community.

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

Johnstown Primary School



e-Safety Policy

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

Development of this Policy

This e-Safety policy has been developed by the Governing Body e-safety sub-committee made up of:

- Headteacher –Mr K McComas
- e-Safety Officer/ICT & DCF Coordinator – Mr D Cousins
- Governors –B Hickman (Teacher Governor), D. Rose(Chair), B. Anderson (Community), N Hopkins (Parent), S. Roberts (Clerk)

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

Schedule for Development

This e-Safety policy was initially approved by the Governing Body e-safety-sub Committee on:	23.05.16
This e-Safety policy was fully approved by the Governing Body on:	
The implementation of this e-Safety policy will be monitored by the:	Governing Body e-safety-sub Committee Senior Leadership Team
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	Annually
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	January 2019
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	School Based Child Protection Officer, LA ICT Manager, LA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents. In the event of a reported incident the school will contact the LA ICT Manager in order to ascertain whether inappropriate content has been accessed on the school network, and to acquire data logs of blocked content as and where appropriate (LA uses smoothwall web filtering policies)
- In the event of a reported incident a request will be made to the LA to send monthly blocked content from the school's Internet activity logs, via email.
- Regular parent and pupil questionnaires (Microsoft Forms/Schoop) related to home Internet usage in order to gain a knowledge of issues experienced by parents at home, which may have an adverse effect on their child/children's wellbeing or on the site's that learners may attempt to access whilst at school (school).

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governor's e-safety sub-committee receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body should assume the role of e-Safety Governor 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 to relevant Governors / sub-committee / meeting

Academic Year 2017-18 Beverly Anderson (Community Governor) has been identified as the e-safety governor to carry out the afore mentioned tasks

Headteacher/SLT:

- The Headteacher has a duty of care for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety may be delegated to the e-Safety Co-ordinator (Mr D Cousins).
- The Headteacher and the Deputy Head Teacher 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 referring to the agreed safeguarding workflow which appears later in this document. (p.22)
- 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 appropriate.
- 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 those colleagues who assume important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the e-Safety Co-ordinator / Officer.

e-Safety Coordinator:

The e-Safety Coordinator

- Leads the e-Safety committee (D. Cousins)
- 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
- Liaises with (school) technical staff
- Receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
- Meets regularly with e-Safety Governor (B. Anderson) to discuss current issues, review incident logs and if possible, filtering / change control logs.
- Attends relevant meeting / sub-committee of *Governors*
- Reports regularly to Senior Leadership Team

Managing the Network:

Johnstown Primary School's Internet Access is provided by the Local Education Authority as part of an on-going Service Level Agreement. Matthew Jenkins (Carmarthenshire ICT Consultant) leads a technical team that ensure that Carmarthenshire schools' internet access is appropriately filtered to block inappropriate, illicit or malicious content. The LA Technical Staff govern the managed service and are responsible for ensuring:

- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the required e-Safety technical requirements as identified by the *Local Authority or other relevant body* and also the e-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- that the filtering policy, compliant with Welsh Government guidelines (provided by Smoothwall and Palo Alto), is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (LA governed).
- that they keep up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant.
- that the use of the network / internet / All Wales Learning Platform (Hwb) , including, but not limited to email, is regularly monitored in order that any attempted misuse can be reported to the Headteacher or e-Safety Coordinator for investigation.
- staff Zimbra email accounts are monitored by the LA technical team so that activity can be investigated in the event of inappropriate use.
- students' email activity is undertaken through Hwb Mail accounts, and this is not within the remit of LA monitoring of email accounts. Subsequently, the designated Office 365 administrator for the school will undertake monitoring of Hwb email activity, in the event of a disclosure/report/incident.

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 or e-Safety Coordinator (Mr. D Cousins) for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems (Schoop/Hwb online resources)
- e-Safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the e-Safety and acceptable use agreements and policies.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches (Internet searches: Google Junior, Hwb Encyclopaedia Britannica and Image Quest).

Safeguarding Designated Person

The designated Safeguarding Officer should be trained in e-Safety issues and work alongside the e-Safety Officer to become aware of the potential for serious safeguarding issues that arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupil e-Safety Group (Y Criw Craff)

Members of the e-Safety Group (Y Criw Craff) will assist the e-Safety Coordinator with:

- supporting peers and adults with new technical advances and software.
- imparting important e-safety messages in relation to online safeguarding and acceptable usage
- publicising safety message on community resources such as safety page on the school website and School

Pupils:

- are responsible for using the school digital technology systems in accordance with 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 on cyber-bullying.
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

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

- digital and video images taken at school events
- emailing
- access to parents' sections of the website / Hwb

Community Users

Community Users who access school systems to comment on blog posts through Hwb (J2Webby/J2Bloggy) as part of the wider school provision will not be permitted to post comments without prior moderation from the school's Hwb Administrator and/or ICT Technician. Appropriate guidance is shared annually with parents when they are requested to sign the Acceptable Use Policy with their child/ren.

Policy Statements

Education – young people

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

e-Safety 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 / Computing / PSE / Digital Literacy lessons (other lessons, as appropriate), and should be regularly revisited. The school will follow the SWGfL Digital Literacy Resource for Wales, available on the Hwb Learning Platform:
<http://onlinesafetycymru.org.uk/home.aspx>

- Following the SWGfL programme of study (POS) will establish an ethos of sharing vital e-Safety messages. These should also be reinforced as part of a planned programme of assemblies, sessions with the school's designated Police Liaison Officer and other timetabled pastoral activities.
- Learners should be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet, especially when their work is shared in public forums with the wider community. This includes, but is not limited to the Johnstown Journal online blog.
- Learners should be helped to understand the need for the Acceptable Use Agreements for using school equipment and online accounts, and also encouraged to adopt safe and responsible use both within and outside school.
- It is the responsibility of the 'Criw Craff' pupil voice council for eSafety to ensure that eSafety messages are consistent across the school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices. This should include, but not be limited to, use of Avatars for profile pictures on education-based online accounts.
- In lessons where internet use is pre-planned, it is best practice that Learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. To reduce the risk of access to unsuitable materials, teacher resourced website links should be shared with learners through J2Launch tiles, live online documents (Office 365/J2E5) or QR Codes.
- Where Learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- It is accepted that from time to time, for good educational reasons, students may need to research topics or access resources that may result in internet searches and/or pages being blocked. In such a situation, the school's eSafety Co-ordinator (Mr D Cousins) may contact the LEA to request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. This can apply to online interactive educational games, which may have been inadvertently tagged as 'online gaming' within the filtering list. 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, School Website, Hwb Learning Platform, AUPs, Schoop
- Parents/Carers eSafety Awareness Evenings, organised and delivered by the school's designated e-Safety Co-ordinator. The School's 'Johnstown Journal', 'Criw Craff' and 'Techi-Tutor' Pupil Voice groups will also help to impart the learning courses to parents.
- High profile events / campaigns eg Safer Internet Day
- Appropriate reference to the relevant web sites / publications eg.
<https://hwb.wales.gov.uk/>
www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

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. The School's 'Johnstown Journal', 'Criw Craff' and 'Techi-Tutor' Pupil Voice groups will help designated teaching staff as they impart the learning courses to members of the wider community.
- E-Safety messages targeted towards grandparents and other relatives, as well as parents.
- The school website will provide e-Safety information for the wider community through a designated e-Safety page.
- As an ERW Professional Learning School for Digital Competence, Johnstown Primary School, its staff and 'Pupil Voice' digital groups (Crew Craff, Johnstown Journalists and Techi-Tutors) are committed to

providing school-to-school support across the consortia region within the areas of Digital Competence and e-Safety.

- Supporting community groups, eg. Carmarthen Senior Citizens in annual events that incorporate digital learning mechanisms. (e.g. Pupils teaching the senior citizens the basics of mobile technologies)

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-Safety as a training need within the performance management process. Inhouse e-Safety training/protocols will be imparted during regular Digital Competence training sessions for staff, which occur weekly during 'Gwasanaeth Gwych' Special Mention Assemblies (Teaching and Support Staff alternating on a weekly basis)
- All new staff should receive in-house e-Safety training, as part of their induction programme. This should include opportunities to read and discuss the e-Safety Policy. This will serve to develop a shared understanding of the school's e-Safety mechanisms and the associated 'Acceptable Use Agreements'.
- The e-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from ERW, SWGfL and/or LA) and by reviewing guidance documents released by relevant organisations associated with eSafety protocols. Any e-Safety training undertaken by the designated e-Safety Coordinator should inform the continual review of the 360 Degree Safe Cymru Self Review Framework (SRF).
- This e-Safety policy and any subsequent updates will be presented to and discussed by staff in staff/phase meetings and INSET days, as appropriate.
- The e-Safety Coordinator will provide further advice, guidance and/or training to individuals, as deemed appropriate by the e-Safety Council (further to eSafety situations that arise).

Training – Governors

Governors should take part in e-Safety training/awareness sessions, with particular importance for those who are members of the E-Safety Council sub-committee.. This may be offered in a number of ways:

- Participation in the in-house e-safety training offered by the school.
- Attendance at parental e-Safety Awareness Evenings/Training Sessions.
- Involvement in lesson observations.
- Attendance at training provided by ERW, LEA or other relevant organisation (eg SWGfL).

Technical – infrastructure, filtering and monitoring

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. Johnstown Primary School is responsible for ensuring that the its network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

As part of Johnstown Primary School's Service level agreement with Carmarthenshire LEA, the designated members of staff responsible for ICT must continually check their Local Authority policies with regard to protocols and procedures related to safeguarding the schools network, user data and equipment.

Responsibilities

The management of technical security will be the responsibility of Mr. D Cousins (Digital Competence and e-Safety Coordinator).

Technical Security

- School technical systems will be managed in ways that ensure that Johnstown Primary School meets recommended technical requirements. These are governed by the Local Authority's policies for internet filtering, equipment and network infrastructure.
- 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 to specified keyholders and those with administrative passwords.
- All users will have clearly defined access rights to school technical systems and devices.
- The LEA school's disk image will be installed on all desktop computers and laptops in the school. This will be assigned with user accounts that have varying permission levels associated with the user credentials. The user accounts include: Administrator, Teacher, Student. The user permissions within each user account are determined by the LEA.
- The "administrator" passwords for the school's ICT systems, used by the Digital Competence Coordinator and ICT Technician, are also be available to the *Headteacher* and other nominated senior leaders (DHT, School Business Manager) and kept in a secure place secure location in the school office.
- The Digital Competence Coordinator is responsible for ensuring that application licences 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. The licences, and deployment mechanisms for the school's mobile devices (iPads & iPods) is undertaken via Apple's Volume purchasing programme and the Cisco Meraki Mobile Device Management (MDM) system. Johnstown Primary School are aware that **inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.**
- Only the designated members of staff with "administrator" privileges/permissions are permitted to download and install software onto the school's equipment. Any software resources must meet the agreed criteria of the LEA's software policies.
- In the event that malware and/or spyware is detected on the school's network or equipment, the LEA Technical support team should be informed immediately in accordance with the school's Service Level Agreement.
- Internet access is filtered for all users. Inappropriate and/or Illegal content are filtered by the Local Authority's 'Smoothwall' web filtering service. The Local Authority retain a log of blocked internet traffic and Johnstown Primary School can request details of these logs, should the need arise. The designated system administrators should contact the LEA ICT helpdesk to report incidents and request filtering changes, should issues arise.
- The school has differentiated user-level filtering based on their user account permission level.
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- In accordance with the Acceptable Use Agreements, staff and learners are made aware of appropriate systems to report any actual/potential technical incident and/or security breach to the school's designated e-Safety Coordinator.
- In partnership with the LEA, appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices 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 'Sophos' virus software.
- A Staff Code of Conduct policy is in place ([please see addendices](#)) which outlines acceptable use of school equipment that may be used out of school, and connected to home network routers.
- Staff without master administration permissions are forbidden from downloading executable files (either downloaded from the internet, retrieved from CDs/DVDs or external storage devices) and installing programmes on school devices. Staff must make a formal request to install any additional software on school devices, and this must be performed by the designated system administrators.
- A Staff Code of Conduct policy is in place, ([please see addendices](#)) which outlines the agreed use of removable media (eg 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.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet.

However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (on social media sites, for example).
- In accordance with guidance from the Information Commissioner's Office, parents/carers are able 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 on social networking sites, nor should parents/carers comment on any activities involving other learners in their photographs or videos.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow agreements concerning the sharing, distribution and publication of those images. Those images or videos should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. Wherever possible, this media should be uploaded to Welsh Government sanctioned Hwb Learning platform (Microsoft Office 365 Onedrive and/or J2Launch cloud repositories).
- Care should be taken when capturing images or videos, to ensure that the learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Learners must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs or video content.
- Written permission from parents or carers will be obtained before photographs of learners are published on the school website.
- Learners' work may only be published with the permission of the Learners and their parents or carers.

Data Protection

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection and/or encryption.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has 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 routines for the deletion and disposal of data in accordance with LEA policies.
- It works in partnership with the LEA's ICT Helpdesk for reporting, logging, managing and recovering from information risk incidents, in accordance with the LEA's policy and the school's Service Level Agreement.
- Agreed use of cloud storage mechanisms are outlined in Acceptable Use Policies and Codes of Conduct, which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office and Welsh Government.

Staff must ensure that they:

- Take every precaution 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 or password protected devices and/or Zimbra briefcases.

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
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, as outlined in this policy document, once it has been transferred or its use is completed.

Password Security

In Johnstown Primary School a safe and secure username and password system is applied for use of any online educational and/or learning platform resources that apply to staff and learners. Desktop computers and laptops have generic passwords to gain access to school systems at varying permission levels. This means that staff who login through the ‘Teacher’ profile will have differences in their web filtering to that of the ‘Student’ profile. Staff will also be able to access system permissions on their devices which would be blocked within the ‘Student’ profile. Only designated members of school staff, in addition to the LEA ICT Technical team, will have access to the ‘Administrator’ profile. Staff have personal usernames and emails to the school’s network drive, LEA governed email service (Zimbra) and the Hwb learning platform. Learners have personal passwords for online accounts, such as Hwb, Bug Club, Times Tables Rockstars and My Maths. Lists of these passwords are kept securely in a locked cupboard within a ‘Password Passbook’ folder. Staff are made aware that these should only be used during the recovery process of a learner’s password for any of their associated online accounts.

Policy Statements:

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the the Digital Competence Co-ordinator (Mr. D Cousins) and will be reviewed. These passwords will be reviewed and updated, further to a need arising from malicious authorisation attempts.
- All staff user logins to the school’s shared network will be protected by secure passwords that are regularly changed.
- The pupils’ digital/resources work will be saved securely through the password protected Hwb online repository (Either in J2E ‘My Files’ (FP and KS2) or Office 365 Onedrive (KS2).
- The ‘master / administrator’ passwords for the school systems, used by the technical staff must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure. Johnstown Primary School will not allow one user to have sole administrator access.
- Passwords for new users, and replacement passwords for existing users will be allocated by Mr D Cousins.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Staff passwords:

- All staff users will be provided with a username and password by the Digital Competence Coordinator (Mr D Cousins) who will keep an up to date record of users and their usernames.
- For best practice, the password should be a minimum of 8 characters long and must include a combination of uppercase characters, lowercase characters and numbers. This is the agreed minimum security requirement for Hwb and Teacher Centre access for staff, and should be replicated across other educational online platforms.
- Passwords must not include proper names or any other personal information about the user that might be known to others.
- Passwords shall not be displayed on screen, and shall be securely hashed
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school. Teacher Centre and Zimbra will automatically request a password change every 90 days.

- Passwords should not be re-used for 6 months and be different from previous passwords created by the same user. The last four passwords cannot be re-used within Teacher Centre and Zimbra.

Student / pupil passwords:

- Students / pupils will be taught the importance of password security
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Use of Cloud Services via HWB

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 for and the ease of 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 volume like email. Schools should consider how to secure and back-up to a local system what could be sensitive or important data.

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 in accordance with 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

Working in partnership with the LEA, there are also safeguarding obligations for the use of technology in schools that include:

- 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

Please refer to the School's Safeguarding Policy for further details and safeguarding mechanisms.

Criminal Activity

Schools have an immediate obligation to report illegal or criminal activity to the Police.

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 to those outside and are more stringent in the detail 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 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 suffers 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?

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, South West Grid for Learning have produced a free Digital Literacy and Citizenship Curriculum for Foundation Stage to Year 10+ which has a variety of strands, one of which focuses on

E-Safety Policy

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.

Monitoring users

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 state 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 “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 both 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 Drives 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.

Mobile Device Management (MDM) via Meraki - 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
- 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?

At Johnstown Primary School, ‘Teacher’ and ‘Pupil’ user profiles are managed centrally via the use of Cisco’s Meraki MDM online system. This allows the designated network managers to control the restrictions and permissions on specific mobile devices across the school.

Apps are also purchased via Apple’s Volume Purchasing Programme and distributed to devices centrally via Meraki MDM.

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, in accordance with government guidance. As part of the school’s Service Level Agreement with the LEA, the Local Authority will undertake the safe disposal of electric hardware containing data.

Communications

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

Communication Technologies	& other adults				Staff				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school (<i>pupils to store mobile telephones in a secure location in the school's office</i>)	X						X					
Use of mobile phones in lessons				X								X
Use of mobile phones in social time	X											X
Taking photos on mobile phones / cameras				X								X
Use of other mobile devices e.g. school tablets	X				X							
Use of personal email addresses in school, or on school network		X										X
Use of school email for personal emails				X								X
Use of messaging apps (Schoop, Office 365)	X					X						
Use of personal social media accounts on school system				X								X
Use of blogs (educational)	X					X						

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and learners or parents/carers (email, Schoop, Hwb 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 KS1, while students / pupils at KS2 and above will be provided with individual Hwb email addresses for educational use.
- Learners 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. *(Facilitated via the SWGfL Digital Literacy Resource for Wales)*
- 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 use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

Unsuitable / inappropriate activities

Some internet activity, such as accessing child abuse images or distributing racist material, is illegal and would obviously be banned from school and all other technical systems. Other activities, such as cyberbullying, would also 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.

Johnstown Primary School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined in the table overleaf, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows (please see table overleaf):

User Actions

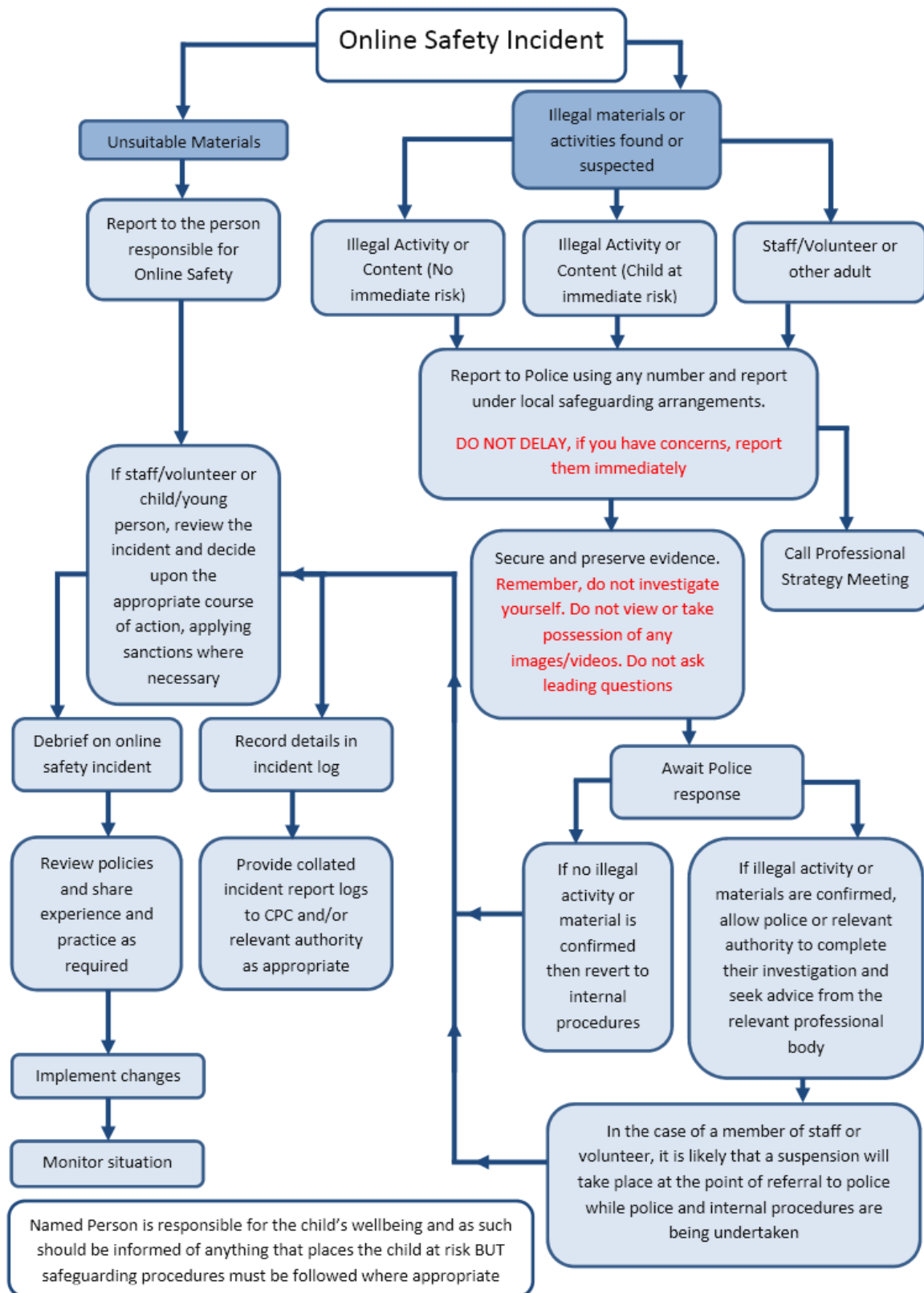
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X		
On-line gaming (educational- such as Times Tables Rockstars, My Maths, Bug Club)	X					
On-line gaming (non educational)				X		
On-line gambling				X		
On-line shopping / commerce			X			
File sharing (via designated cloud-based platforms such as Office 365 and/or J2Launch)	X					
Use of social media				X		
Use of messaging apps (such as Schoop)	X					
Use of video broadcasting. E.g. Youtube for educational content only		X				

Responding to incidents of misuse

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

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

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

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

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

It is important that all of the above steps are taken, as they will provide an evidence trail for the school, and possibly the police, and demonstrate that visits to these sites were carried out for safeguarding purposes. Any subsequent Safeguarding forms that are completed in relation to an incident should be retained by the e-Safety Sub-Committee 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. At the discretion of the Senior Leadership Team, reported e-Safety incidents should be discussed in E-safety Council Sub-committee meetings. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures, as follows (please see table overleaf):

Students / Pupils

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

Staff

Actions

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

Appendices – Section A - Acceptable Use Agreements

• Staff - Communications Code of conduct (younger children)	26
• Pupil - Acceptable Use Agreement for Hwb (FP Learners)	27
• Pupil - Acceptable Use Agreement for Hwb (KS2 Learners)	28
• Staff - Acceptable Use Agreement for Hwb	29
• Parent - Acceptable Use Agreement Letter for Hwb	30
• Parent - Acceptable Use Agreement Letter for Digital Learning	31
• Pupil – e-Safety posters (FP Learners)	32
• Pupil – e-Safety posters (KS2 Learners)	33

Appendices – Section B – Support documents and links

• Staff – Training Needs Audit template	34
• Summary of Legislation	35
• Links to other organisations and documents	40
• ERW Dealing with adverse comments and complaints against schools on social media	42



Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Head Teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- School equipment connected to home wi-fi networks must adhere to the school's internet Code of Conduct, i.e. No websites should be visited at home which would be deemed inappropriate and blocked by the Local Authority's web filtering system.
- I am aware that I must never associate school devices with personal accounts, for the purpose of downloading applications that do not have an educational purpose (including, but not limited to, iPads).
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware on school equipment without software licenses or the permission of the ICT Co-ordinator and/or Senior Management Team.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Any removable storage (pendrives) must be encrypted and/or password protected.
- I will respect copyright and intellectual property rights, particularly when digital material is shared with a wider audience via the Internet, social media or online cloud repositories.
- If I hold personal social media memberships (including, but not limited to, Facebook, Twitter, Flickr), activity must conform with my professional role - where references to, and digital media from, school are never associated with my personal account/s.
- I understand that it is improper to capture digital media from school on a personal device, including, but not limited a personal mobile telephone.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator (Mr D Cousins) and the Child Protection Coordinator (Mr K McComas).
- I will ensure that any electronic communications with pupils conform with my professional role.
- I will promote e-safety with students in my care, and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed:	Capitals:	Date:
Accepted for School:	Capitals:	Date:

Hwb+

Hwb+ is a cool school tool!

Please remember to follow the eSafety rules:

- Be polite when you're online - don't upset or bully anyone .
- If you feel upset or bullied, tell a teacher or adult right away.
- Be safe – don't tell anyone where you live, where you are going or what your phone number is.
- Be security smart - keep your email, username and password safe.
- Check with your teacher or an adult you trust before you send any emails.
- Only open emails from people that you know.
- **I understand that all of my work can be seen by my teacher.**

I understand that I must follow these rules or I might be in trouble.



I agree with what I have read above and/or what my teachers have told me about using Hwb+ properly.

Name of child: _____ Date: _____

Child's Signature: _____ Class: _____

Parent's Signature: _____

Remember, anything you do on your Hwb+ Learning Platform should have an educational purpose. Follow these important eSafety rules:

- Be polite - never post something online on Hwb+ or send an email which is likely to cause offence to someone else. Don't upset or bully anyone.
- Be careful what you say and how you say it. What you do and say on Hwb+ is recorded and will be viewed by other people including your teacher.
- Be safe – don't reveal anything about yourself or about your friends (especially home addresses or phone numbers). **This is very important.**
- Be security smart - keep your email, username and password safe.
- Protect the school community by telling a teacher if you see anything that might cause upset or harm to yourself, other pupils or teachers in the school.
- Only link to other websites if you are sure they are safe to visit, have been approved by a trustworthy adult and are appropriate for your age.
- Send emails as directed by your teacher – don't communicate with people you or your teachers don't know. Don't open emails if you don't know the sender. If you are unsure, always check with your teacher. Email use may be monitored.
- Don't upload anything to the platform that you would be happy to share with your teacher.
- **I understand that all of my work can be seen by my teacher.**

Your school may have to look at taking you offline if you break any of these important rules. They are for the good of everyone, yourself included.



I agree with the Acceptable Use statements above.

Child's name: _____ Date: _____

Child's Signature: _____ Class: _____

Parent's Signature: _____



Acceptable Use of Hwb+ for School Staff

Remember, anything you do on Hwb should have an educational purpose. You should not regard any of your activity as private or confidential.

- Be a positive role model for your learners in how you use Hwb+.
- **Keep your username and password safe. You are responsible for anything that happens within your account.**
- Report to your Hwb+ administrator if you suspect that your username and password have been compromised.
- If you share external links within Hwb+ then you deem that the content of the external website is age appropriate and has an educational purpose. *E.g. a Youtube link*
- You may not access, distribute or place on Hwb+ material that is in breach of the statutory rights of copyright owners.
- Protect the school community by reporting anything you see that might cause upset or harm to yourself, other teachers or learners in the school. You are expected to demonstrate a professional approach and respect for pupils and their families, and for colleagues and the school.
- Creation or transmission of any offensive, obscene or indecent images, data or other material is prohibited. Content relating to or supporting illegal activities may be reported to the authorities.
- Personal use of your mailbox and cloud storage is to be avoided. Emails may be monitored
- ***Always keep another local copy of your essential work that you store on the cloud.***

Unacceptable use within Hwb+ (as highlighted but not limited to that above) might result in actions taken in line with the school's Disciplinary Policy.

Cross out as appropriate.

I do/do not agree to the Terms of Use as outlined above.

Name of teacher: _____ Date: _____

Signature: _____

Dear Parent/Guardian,

ICT – HWB+ at Johnstown School

In December, 2012 the Minister for Education and Skills, Leighton Andrews launched a new initiative in Wales which would support improvements in outcomes for all learners. The initiative was to develop a world class Virtual Learning Environment (VLE) across Wales called Hwb.

Each school is to have its own VLE (called Hwb+) accessible for teachers and learners in the short term and accessible for parents and the wider community in the longer term. Different features of the VLE are supplied by different companies:

- **Learning Possibilities** - the Hwb+ website itself and learning tools
- **Microsoft** – The Microsoft Office Suite online (*including Word, Powerpoint, Excel and OneNote*), Cloud storage and email.
- **J2 Launch** – A Suite of online web tools, resources and cloud storage to assist with your child/children’s ICT acquisition and holistic learning experience.

We believe in the power of ICT to enthuse, engage and motivate learners to achieve their full potential. We live in a technological world and its essential that your child develops a range of ICT skills within a safe learning environment. The *HWB+ All Wales Learning Platform* is a “*Walled Garden*” which will enable your child to embed these skills safely.

Attached is our child friendly HWB+ Online Safety policy, which we are asking you to read carefully with your child, sign and return to school.

We will be offering further eSafety awareness sessions for families in the Spring Term.

Thank you for your support.

Yours Sincerely

Head Teacher

Hwb+

Dear Parent/Guardian,

As part of the National Curriculum and the school's ICT programme of study, Johnstown Primary School provides pupils with supervised access to the World Wide Web. This includes (but is not limited to) access to a wealth of online learning tools within the Hwb Learning Platform. Hwb has been created and is fully endorsed by the Welsh Government as a sanctioned online repository of digital tools that enable learners in Wales to access skills that conform to the curriculum and the requirements of the ICT Framework. All pupils must obtain parental permission before accessing resources online, and we kindly request that you read and return the enclosed documentation as evidence of your approval, and your child's/children's acceptance of the school's eSafety rules.

Access to the World Wide Web enables pupils to access a wealth of information and resources, as well as the possibility to collaborate and exchange digital content. It also provides a means for the school and pupils to store their work in an online cloud and celebrate their achievements by publishing information and examples of work to a wider audience via the school's website, for example. However families need to be mindful that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst school access to the Internet is curriculum based, filtered and well supervised, pupils may attempt to find ways of accessing other materials as well. We believe that the benefit of online learning exceeds any disadvantages. Ultimately, parents and carers are also responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

In school teachers or suitable adults will guide pupils toward appropriate online materials and ensure that online learning conforms with pupil safeguarding and any guidelines outlined in the school's eSafety Policy. Outside of school families bare the same responsibility for such guidance and safeguarding. Parents should endeavour to exercise the equivalent level of caution with use of the Internet and Social Media as they would normally consider with other information sources, such as television, telephones, movies, radio and other potentially offensive media.

We would be grateful if you would read the enclosed materials and then complete the attached permission documentation before returning it to school at your earliest possible convenience.

Yours sincerely

Headteacher

Think then Click

These rules help us to stay safe on the Internet



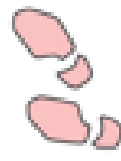
We only use the Internet when an adult is with us.



We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.



We always ask if we get lost on the Internet.






We can send and open emails together.



We can write polite and friendly messages to people that we know, using a computer.

Think then Click

e-Safety Rules for Key Stage 2

-  We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
-  We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
-  We do not use Internet chat rooms in school.

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's 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 person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with 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 a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing 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 other 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, in order 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 or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks 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 copyright 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, and 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 to a fine or to 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 with the intention of committing 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, 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 particular 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

Office 365 through HWB – further information

Where is the data stored?

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

How often is the data backed up?

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

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

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

How does the email provider protect your privacy?

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

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

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

Who has access to the data?

By default no one has access to customer data within the Office 365 service. Microsoft employees who have completed appropriate background checks and have justified need can raise an escalation for time-limited access to Customer data. Access is regularly audited, logged and verified through the ISO 27001 Certification.

As detailed in a recent accreditation submission to the UK Government, any organisation that specify “UK” as their country during tenant creation will be provisioned and data stored within the EU datacenters (Dublin and Amsterdam).

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

Schools may wish to consider the extent to which applicable laws in the US – which apply to services operated by companies registered in the US, e.g. Microsoft and Google – affect the suitability of these services. For

example the US Patriot Act provides a legal means through which law enforcement agencies can access data held within these services without necessarily needing the consent or even the knowledge of the customer. Whilst SWGfL doesn’t intend to put anyone off getting value from these beneficial services we feel it’s only right to share what we know about them.

Is personal information shared with anyone else?

No personal information is shared.

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

No. There is no advertising in Office365.

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

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

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

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

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

How reliable is the email service?

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

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

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

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 direct on their [UK Schools Cloud Blog](#).

Links to other organisations or documents

Johnstown Primary Home/School Agreement:

- Please click on the link provided to view the [Home School Agreement](#) for Johnstown Primary School.

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](#)

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!"](#)

Dealing with adverse comments and complaints against schools on social media

**Cynghrai o 6 awdurdod lleol yw ERW a reolir gan gyd-bwyllgor cyfansoddiadol cyfreithiol.
Y nod yw gweithredu strategaeth a chynllun busnes rhanbarthol cytunedig a chefnogi gwelliant ysgolion.**

ERW is an alliance of 6 local authorities governed by a legally constituted joint committee.
Its aim is to implement the agreed regional strategy and business plan to support school improvement.



1. Introduction

The increasing number of people using social media has had both a positive and an adverse effect on the reputation of schools in local communities. Some schools have used it as an efficient tool, e.g. to communicate information through Facebook and Twitter. Stakeholders have responded well to this dialogue.

However, in some cases, individuals have bypassed a school's complaints procedures and instead used social media to criticise and, in some cases, make malicious comments about individual members of staff or decisions that have been taken by the Headteacher or governing body.

In many ways the use of social media to express these opinions is an extension of how people can express their views more widely on the internet. People use sites such as "Trip Advisor" to review holiday accommodation and "Amazon" to give assessments of particular products. However, remarks made about a school can be destabilising for a community and, in particular, for the professional status of staff members who have had allegations made against them. It can also lead to a "whispering campaign" which can undermine the leadership of the Headteacher and the governing body.

The key question is, "how do schools respond to complaints made on social media?"

There is no single effective method of dealing with individuals who raise issues on social media. However, schools can take a proactive approach to minimise such incidents rather than having to always be reactive.

If the complaint is of a low level and if no staff member is named which links adverse comments to individuals then it may be best not to respond in order that the matter is not prolonged. It should be noted that people have a right to freedom of expression under the Human Rights Act 1998. This includes freedom to hold opinions, and to receive and impart information and ideas without interference by public authority.

This short guide gives details of a number of processes a Headteacher can use to deal with contentious comments; it also looks at ways to counter any repeat occurrences to ensure that individuals are encouraged to follow established complaints procedures.

2. Gather Evidence

When the school becomes aware of any information that is damaging towards an individual member of staff and/or the school community, it is important to gather evidence and establish what has been posted. This may have to be done through various methods as the information may have only been shared through the connections of specific people. However, it is important that verbal or written evidence is gathered so that the facts can be established.

In some cases, a group of parents may set up a site to criticise the school or individual members. This is usually done through a Facebook page which is then "liked" by those with an account and discussions then take place through particular threads. In this case, it is important to find out who has set up the page, as usually this is the individual who has the grievance.

It is also essential, at this stage, that members of staff (including non-teaching staff) do not become embroiled in any of the discussion threads as this sometimes can inflame the situation.

3. Reassure Staff

The appearance of comments on social media that make allegations about the school or individual members of staff can be very intimidating to the workforce. Sometimes the content of the posts can de-motivate staff and cause anxiety. It is, therefore, vital that the Headteacher reassures all staff and offers support through whole-staff meetings or individual discussions. It is also essential that staff have access to their local trade unions who may be able to offer additional support and further services to members.

In some cases there may be malicious allegations made about a member of staff that needs to be investigated, for example, a suggestion that a child or young person has been manhandled by a staff member, and the Headteacher will have to use the school's safeguarding procedures to carry out a formal inquiry into the matter.

4. Meet with Individuals

In many cases the reason why an individual has made comments about the school or staff members on social media has either been through ignorance about the implications of making such comments or that they are unaware of the school's complaints procedure. In the majority of incidents a meeting with the individual can resolve the matter and the Headteacher can identify the particular grievance and ensure that a suitable solution is put into place, if necessary via the school's complaints procedure. At this meeting it is helpful if printouts of the allegations or comments are available to verify what has been posted. At this stage, it is important that the Headteacher asks that any offending posts or pages are removed from the site.

In cases where malicious comments or allegations have been made and the meeting is not successful the Headteacher may need to take further action.

5. Further action

If the matter is not resolved at this meeting, then the school has a number of options to address the situation. While it does not want to escalate the matter, it is crucial that it tries to come to a sensible conclusion.

a. Arrange a further meeting and invite the chair of governors and/or a relevant local authority officer.

To ensure that the individuals understand the seriousness of the matter, a further meeting can be arranged with the chair of governors and/or a relevant local authority officer present to convey the damage that these comments are having on the school community. This gives a further opportunity for the individuals to share their grievances and for an action plan to be established which could include proceeding with a formal complaint.

b. Report offending material

If the individuals do not agree to remove any offending content or pages they have set up, then the school can report offending material to the site administrators. Usually this raises a "ticket" with those who monitor content on the site and they assess this in relation to whether any of the terms and conditions has been violated. Schools should be aware that there will be a time

delay in the review of this content and that; if the content does not breach the terms and conditions, then the site administrators will not remove it.

Material can be reported through the following processes:

Facebook – www.facebook.com/help/181495968648557/

Twitter – www.support.twitter.com/groups/56-policies-violations/topics/238-report-a-violation/articles/15789-how-to-report-violations

YouTube – www.support.google.com/youtube/?hl=en-GB&topic=2676378#topic=2803138

c. Take legal advice

In serious cases the school may wish to seek legal advice. In some cases this has resulted in a letter from a solicitor being sent to the individuals warning them that malicious allegations could result in legal action.

d. Consult the police

In the most serious cases the police may consider a prosecution under the Malicious Communications Act 1988.

6. Assure Parents

Allegations or malicious comments against members of staff or the school can have a negative impact on the school community.

If the comments appear to be one off or an isolated incident, the school may wish to make a low level response which avoids escalation. The Headteacher may put some wording in the school newsletter to remind parents/carers in general terms about appropriate use of social media and the correct procedures for raising concerns with the school. Here is some suggested wording:

“As a school we are working very hard to be approachable and to ensure that as parents you are an important part of your children’s education. If you feel that something has been mishandled then please do come in to see us about it. We promise that we will take your concerns seriously. Please could I ask that you come in and discuss any problems with the appropriate member of staff and not to use Facebook or other digital media to air a grievance. It really is hugely discouraging for staff, has a potentially massive audience and worst of all does not afford us with an opportunity to respond.”

If the comments are of a more serious or sustained nature the school could send a letter to parents/carers along the following lines:

“Dear Parent/Carer,

As you will be fully aware, the internet has become a powerful tool to connect and to share ideas and opinions. In recent years, social media such as Facebook have grown in popularity and many people use them to communicate with family, friends and others.

The vast majority of people who use social networking show respect in their communication with others and this is something that we must encourage to show our children that we are positive “digital role models”.

However, like other aspects of society, there are people who disregard the rules set and will use social media inappropriately.

As a school, we encourage parents to support us with the education and wellbeing of their children. If at any time parents feel that they have issues regarding their child's education, they should make an appointment with me. As a community, we should discourage the use of social media to criticise and make unsubstantiated comments about the school or any members of staff.

(If appropriate) In light of this, I have updated the current "home-school agreement" to include a section about the school's complaints procedure and I would be grateful if you could read, sign it and return it to school.

(If appropriate) Also, I am arranging a parent session on e-Safety to help us support our children in the online world. More details will follow shortly.

Thank you for your continued support.

Regards,
Headteacher and Chair of Governors"

7. Other action

a. Home-school agreement

Schools have a contract with parents to ensure that children and young people are fully supported with their learning and welfare both inside and out of the classroom. Many of the statements refer to parents reinforcing schools' policies on homework, behaviour and conduct. In order to counter discussion of sensitive issues about individual teachers or pupils on social networks, a number of schools have decided to include a statement on the home-school agreement to try and stop parents from making derogatory or malicious comments. While it is not practical to monitor parents' use of social media, it does show that the school takes this matter seriously and, the fact that parents have signed the agreement, means that they have a responsibility to act appropriately. Some example statements are as follows

"Parents/carers are reminded to use the schools complaints procedure when making a complaint about the school or a member of staff. They are advised not to discuss any matters on social media".

"If at any time during your Childs education at xxxx school, you wish to make a complaint, then you are advised to follow the school's complaints procedure which can be found on the school website [insert link]. We recommend that all parents and carers refrain from using social media to discuss sensitive issues about the school".

"As a parent, I support school policies on ICT and I will ensure that I monitor my Childs use of the internet (including social media) outside of school. I will act as a positive role model to my child, by ensuring that I use social media responsibly".

b. Complaints policy

Schools are required by law to have a complaints policy.

8. Staff

On the rare occasions where staff members make inappropriate or damaging comments about the school on social media, the general principles outlined in this document will apply, but in serious cases it may be necessary to take action through the schools disciplinary procedure.

Conclusion

In the age of social media, all institutions need to be robust against criticisms. Complaints by parents are nothing new for schools as, in the past, many have gone to local media outlets such as newspapers to highlight decisions or issues made by the school. The problem today is that these complaints can easily be shared in the public domain and a post on Facebook can reach thousands of users instantly and give a misleading slant to any issue. Schools cannot monitor every comment put on social media, but they can be proactive in trying to ensure that parents and carers have a responsibility to act as a positive digital role model" to their children.

With thanks to:

Yorkshire & Humber Grid for Learning and Surrey County Council