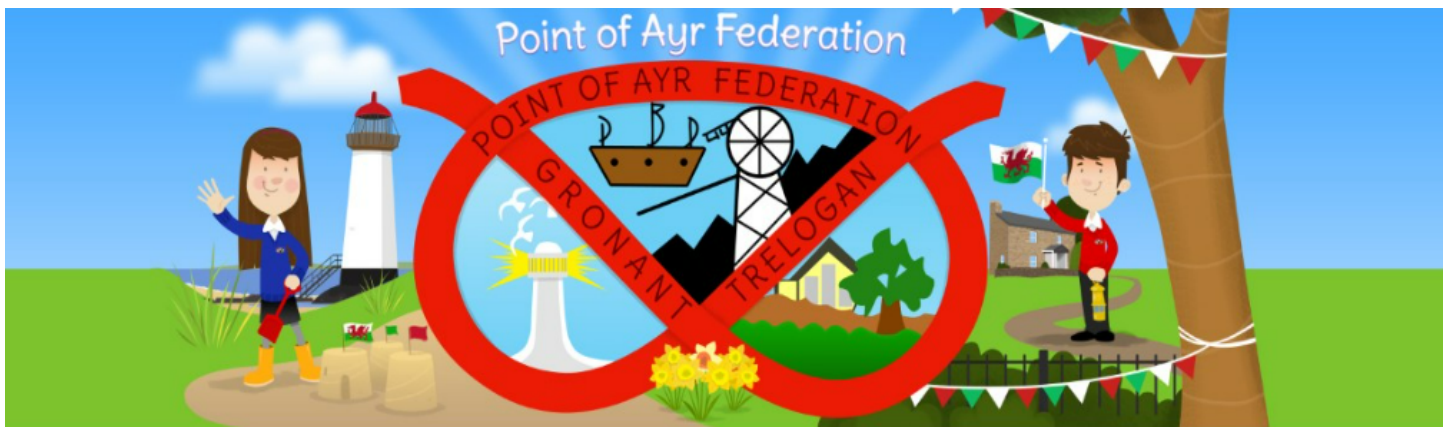




Point of Ayr Federation

Online Safety Policy November 2022



Aiming High Together

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

The Point of Ayr Federation has identified the need to embrace the use of digital technology in order to equip our pupils with the digital competencies to access lifelong learning and enhance their employment opportunities in the future. At The Point of Ayr Federation, learners will learn to be conscientious digital citizens who contribute positively to the digital world. They will be prepared for and ready to encounter the positive and negative aspects of being a digital citizen and will develop strategies and tools to support them as they become independent citizens.

Roles and Responsibilities

Online safety is an important aspect of strategic leadership within the school, the Digital Leader, Headteacher and Senior Leadership Team have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Digital Leader is responsible for coordinating online safety at The Point of Ayr Federation, and keeping all staff updated. All Governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Online Safety and staff

- All staff receive regular updated information and training on online safety issues when required from the Digital Leader, Headteacher and/or outside agencies.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety, and know the reporting procedure for any concerns.
- All staff have agreed to and signed the school's acceptable use agreement. (See Staff Acceptable Use Agreement section within the **Acceptable Use Policy**)
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Disciplinary action could be taken if they are found to bring the profession or school into disrepute.

Online safety and learners

- All learners must sign a Learner's Agreement via the **Photographs and Digital Communications** form.



Aiming High Together

- All parents/guardians must sign a Parental Agreement with regards to understanding and accepting the agreement that their child has made, via the **Photographs and Digital Communications** form.
- Delivery of digital citizenship is a cross-curricular responsibility as part of the Digital Competence Framework.
- Learners will partake in annual Digital Citizenship weeks.
- Learners will partake in Online Safety sessions delivered by the School Community Police Officers,

Community use of the internet

- External organisations using the school's digital facilities must adhere to this Online Safety policy.

Cyberbullying management

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details and procedures are set out in the school's anti- bullying and behaviour policy.

Managing Internet Access

Email

Email is an essential means of communication for both staff and pupils. The Point of Ayr Federation believes that learners should be taught how to use email positively and responsibly.

- Pupils may only use the email account linked to their HWB Account account which can be monitored by the Digital Lead and Headteacher.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers.

Published content and the school website



Aiming High Together

The contact details on the website are the school's addresses, emails, Twitter handles and telephone numbers. Staff or pupils' personal information will not be published. The Headteacher, Assistant Headteacher and Digital Lead will take overall editorial responsibility and ensure that content is accurate and appropriate.

Online Safety and parents/carers

● Parents/guardians are required to make a decision as to whether they consent to images of their child being taken and used online e.g. on the school website, blogs, Twitter. Parents/guardians are required to sign the **Photographs and Digital Communications** form.

Publishing learner's images and work

● Images or videos that include pupils will be selected and used appropriately, in line with our **Photographs and Digital Communications** consent form and 'Conditions of Use'.

● As outlined in our **Photographs and Digital Communications** consent form, parental and child consent is considered valid for the entire period that the child attends our school, unless there is a change in the child's circumstances where written consent will be required. Parents/carers may withdraw permission, in writing, at any time.

Photographs and Digital Communications Conditions of Use:

1. This form is valid for the duration of your child's registration at school.
2. We will not re-use any photographs or recordings after your child leaves compulsory education.
3. We will not re-use personal details or full names (which means first name and surname) of any child or adult in a photographic image on video, on our website, in a prospectus or in any of our other printed publications.
4. We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, in a prospectus or in other printed publications.
5. If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption.
6. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.



7. We may include pictures of pupils and teachers that have been drawn by the pupils.
8. We may use group or class photographs or footage with very general labels, such as 'a Science lesson' or 'making Christmas decorations'.
9. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will insist that photographs/videos taken are of their own children only. Photos/videos that include images of other children must not be shared online unless permission has been granted from the parents of the other children.

Social networking and personal publishing

- The school and county firewalls will block access to certain social networking sites to pupils.
- Pupils and parents will be advised that the use of many social network sites outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them and we will advise them on how to keep safe whilst using these sites; e.g. powerful passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils are asked to report any incidents of cyberbullying to staff. All incidents are logged.
- School staff are strongly advised NOT to add past or present pupils as 'friends' if they use these sites.
- Concerns regarding learners' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning learners' underage use of sites.

Managing video calls

- Learners are not permitted to partake in any video calls that have not been agreed to by parents and staff.



Aiming High Together

- Learners and staff will not make use of video call technology that is not a trusted Hwb platform, such as Google Meet and Microsoft Teams. E.g: Use of FaceTime, Skype, Zoom etc is not permitted.
- In the event that a video call may be used to enhance learning, it must be, pre-arranged by a member of teaching staff, be, under direct supervision and in line with our **Blended Learning** policy and **Live Lesson, Online Learning** policy.

Managing Video Calls for Remote and Blended Learning

- In the event where staff want to undertake an Online Live Streaming/Video Conferencing to their learner, teachers will follow the guidance set out in our **Blended Learning** policy and **Live Lesson, Online Learning** policy.
- Staff are required only to use platforms through HWB tools such as Microsoft Teams or GoogleMeets in G-Suite for Education. Parents are required to complete the **Photographs and Digital Communications** consent form, therefore agreeing to and following guidelines and procedures on behalf of themselves and the learner.
- Guidance for Staff regarding managing video calls for remote and blended learning can be found via Hwb.

[Live Streaming Safeguarding Principles and Practice for Education Practitioners](#) (Updated 08.03.21)

Remote Learning

The Point of Ayr Federation has identified that Seesaw, HWB and GoogleClassroom in G-Suite for Education are safe ways to communicate with learners and provide home learning. 'How to' videos and help sheets have been provided via the website to ensure that learners and parents are able to navigate through the platforms safely. All platforms require the learners to log in using the individual usernames and passwords or individual home learning codes.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and an informal risk assessment will be carried out before use in school is allowed.
- Staff are expected to use cloud based storage via their Hwb accounts (rather than memory sticks, external hardware devices etc, to avoid loss of personal data related to staff or pupils. (See data protection procedures)



Aiming High Together

● Pupils are strongly advised NOT to bring personal mobile devices/phones/smart watches to school – unless there are exceptional circumstances. Any phones that are brought to school are handed in to the class teacher and kept until the end of the day.

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be managed by Flintshire County Council.
- Security strategies will be discussed with Flintshire County Council.
- Personal data taken off site must be secure, saved in the cloud, and devices must be password protected.
- Files held on the school's network are subject to checks by members of the Senior Management Team.

Managing filtering

- Flintshire County Council provides a filtering service for all Chromebooks, desktop computers, laptops and iPads. Filtering follows Welsh Government guidelines
- Both filtering systems will block all sites considered inappropriate.
- Changes to the school filtering policy will be risk assessed by the Headteacher and Digital Lead.
- All breaches of filtering will be reported to the Headteacher if necessary. Staff and pupils are aware of this procedure.
- Our Flintshire County Council ICT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Protecting personal data

See Data Protection Policy

Password Security



Aiming High Together

- Staff are provided with an individual network and Flintshire County Council login username and password which can be accessed from all school provided laptops and desktop computers. Staff are expected to keep these passwords safe and secure, are not permitted to share log ins with others, and must not write passwords down where it is possible that someone may gain access to it. Staff should make use of Hwb/Google Keep to store passwords safely and securely.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network. Administrator passwords are controlled by Flintshire County Council on networks accessed via desktops and laptops. For all other systems administrator passwords are controlled by the school secretary.
- Staff are provided with a Hwb account and Seesaw account, which can be accessed from any device. Devices must be password protected. Staff are expected to keep these passwords safe and secure, are not permitted to share log ins with others, and must not write passwords down where it is possible that someone may gain access to it. Staff should make use of Hwb/Google Keep to store passwords safely and securely. For these systems administrator passwords are controlled by the Digital Lead.
- Learners have individual Hwb accounts, Seesaw Home Learning Codes and IDL accounts and passwords. Younger learners have access to their Digital Toolkit, and as agreed to in our **Acceptable Use Policy**, via our **Photographs and Digital Communications** consent form, will keep their Digital Toolkit safe and secure, and will not share it, nor will they try to use any other person's usernames and passwords. Learners understand that they should not write down or store a password where it is possible that someone may gain access to it, and agree to storing passwords via Hwb/Google Keep and discontinue use of my Digital Toolkit when they are confidently able to do so.
- Learners have access to Seesaw Home Learning Codes which grants them access to their own Seesaw journal. Learners may add to their journal, complete activities, and receive messages/announcements from their class teacher, Digital Lead and Headteacher. Learners are not able to access the journals of their peers, thus protecting their personal identifiable information, such as; names, photos, videos, or voice recordings.
- Learners have access to a Class Code to make use of Seesaw within the school building only. The Class Code enables learners to work together, and allows them to view and make comments on each other's journals. As a Federation, we recognise the importance of learners working together to enhance learning opportunities, and have therefore identified minimal risk to learners data protection, due to Seesaw's own robust privacy policy. (See **Acceptable Use policy**). Learners understand that this Class Code must only be used within school, and must not be shared or used outside of the school building, in line with our **Acceptable Use policy**.
- Pupils are not allowed to deliberately access online materials or files on the school network, or on the devices of their peers, teachers or others.



Aiming High Together

Handling online safety complaints

Complaints of internet misuse will be reported to the Headteacher. All incidents will be logged and kept in the Incident file, in the Acting Headteacher's office. Complaints of safeguarding must be dealt with in accordance with school safeguarding procedures. Pupils and parent's complaints procedures are available to pupils and parents on request.

Monitoring and review

This policy, supported by the school's Acceptable Use Agreement, Blended Learning Agreement, Live Lesson and Online Learning agreement via the Photographs and Digital Communications consent form, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for ICT/Digital Learning, Home-school agreements, Behaviour, Safeguarding, and PSHE policies including Challenging Bullying.

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Headteacher and Digital Lead. The adherence of this policy is the collective responsibility of the staff.



Reporting of an Online Safety incident:

