e-Safety Policy

This policy outlines the acceptable use of the Internet and related technologies

September 2022

Date discussed with Staff:	Date discussed with Governors:
Date ratified by Governors:	
Date for review:	
Signed:	Headteacher
Signed:	Chair of Governors

Heygarth Primary School
e-Safety Policy

1.1 Introduction to E-Safety

The term E-safety covers the issues relating to young people and staff and their safe use of the Internet, mobile phones and other electronic communication technologies. This policy assesses the protocols for ensuring that these initiatives are carefully developed in our school, so that we progress responsibly and appropriately in the interests of our children. It also looks at how we educate our children to be safe in a world where technology is so readily available.

At Heygarth Primary School, we celebrate the value and importance of technology in our children's learning. In our school; iPads, wireless laptops, digital voice recorders and digital cameras are all part of children's everyday learning. The internet has become a vital source of learning and communication for all members of our school community.

Pupils interact with new technologies and the Internet on a daily basis and experience a wide range of opportunities and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

Our school seeks to provide the right balance between controlling access, setting rules and educating students for responsible use.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- A well thought out approach regarding how to develop E-Safety guidance within the school's curriculum.
- Identified opportunities to ensure that we support families with the challenges relating to E-Safety in the digital age (family workshops, web-links etc).
- Secure, filtered broadband from Virgin Media;
- A school network that complies with the National Education Network standards and specifications.

1.2 E-Safety and the Legal Issues

E-safety should be applied to protect children, staff and all members of our school community. Our School's e-Safety Policy replaces the Use of the Internet and Email Policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. Pupils must also learn that publishing personal information could compromise their security and that of others.

Heygarth Primary School will make it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". We will also ensure that all reasonable actions have been taken and measures put in place to protect users.

In practice this means that this school ensures that;

- It has effective firewalls and filters on our school network.

- Ensures that e-safety responsibilities are clearly communicated to all members of our school community.

- That our e-safety policy is fully enforced for children, staff and visitors.

- Ensures that our procedures are consistent with Data Protection laws (specifically the General Data Protection Regulation and Data Protection Act 2018).

Learning and Teaching in the Digital Age

The school uses wireless laptops and iPads and comprehensive broadband access to develop learning and teaching through digital communication. Access to instant messenger services and mobile phones is not allowed as part of this school's curriculum. However, the school will include provision to educate children how to use this technology appropriately and safely.

2.1 Why the Internet and digital communications are important

Mobile Communication equipment and the Internet are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. We also recognise that children are actively engaged with digital communication form an early age. It is part of their lifelong learning experiences and habits. However, we also have a responsibility to ensure that our children learn to use these opportunities and resources responsibly, appropriately and productively to enhance their learning.

In addition, use of the Internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Encouraging responsible use of the Internet and digital communication

1. The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils. We encourage the use of a school-safe search such as http://www.safesearchkids.com/

2. Pupils will be taught about responsible and appropriate information sharing through the internet and other forms of digital communication.

3. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

4. Pupils will be taught about responsible use of e-mails and other sources of digital communication including e-mail, messenger services and texts.

5. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

6. Pupils will be shown how to publish and present information to a wider audience safely and responsibly.

2.3 Pupils will be taught how to evaluate Internet and other digital communication content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.

- Pupils will be taught how to report unpleasant Internet or other digital content including messages, e-mails and texts.

- Pupils will be taught how to safely use Makewaves, a school safe social network designed especially for education and school broadcasting. Only students and their DBS checked teaching staff can join. Makewaves follows the Home Office Task Force on Child Protection Guidance. They are registered with the Family Online Safety Institute and work closely with organisations such as Childet International and SAFE (www.safesocialnetworking.org) to provide safety information for students and parents. Through using Makewaves, it will teach pupils how to manage the risks and dangers associated with other social networking sites.

3. Managing Digital Access, Communication and Content

3.1   Information system security
- School ICT systems security, virus protection and security strategies will be reviewed regularly by Hi-Impact Consultancy.

3.2   Managing filtering
- The school will work with the Local Authority to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the member of staff

3.3   Online Communication
- Staff should only use school approved e-mail accounts at work. Clear guidance for what constitutes professional use of e-mail is included in the Acceptable Use agreements. However, we are absolutely clear that staff cannot use e-mail to communicate personal opinions that may be defamatory or abusive to individuals or organisations associated with the school.

- Pupils must immediately tell a teacher if they receive offensive messages.

- In online communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The forwarding of chain letters is not permitted.

3.4   Published content and the school web site
- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or a senior member of staff.

- The head-teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.5 Publishing pupil's images

- Photographs that include pupils will be selected carefully. The school will always risk assess/review photographs for possible abuse.

- Pupils' full names and other personal details will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

- Written permission from parents or guardians will be obtained before photographs of pupils are published.

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.   Guidance @ Children, Families, Health and Education Directorate page 6 June 2008

3.6 Social networking and personal publishing

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- Staff are fully informed of their responsibilities regarding the use of social networking sites such as Facebook or Twitter. At Heygarth Primary School we have agreed that it is good practice to separate professional and personal commitments. Therefore, the following groups should not be allowed as contacts and friends on social networking sites;

  - **Ex-pupils or current pupils** - the context of teacher to pupil relationship is not suitable for social networking.
  - **Parents** - We believe that it is unfair on parents and staff to complicate the professional relationship that exists within school through the use of social networking sites. It is both inappropriate and open to abuse.

- All staff are also aware that they could face charges of gross misconduct if they use social networking platforms to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.

- Staff are also aware that they are responsible for the security protocols regarding any social networking accounts. This is a professional responsibility.

NEU Cyber-Safe guidance states all staff should;

- Not post information and photos about themselves, or school-related matters, publicly that they wouldn't want employers, colleagues, pupils or parents to see;

- Keep passwords secret and protect access to accounts;

- Not befriend pupils or other members of the school community on social networking sites. (Staff should consider carefully the implications of befriending parents or ex-pupils and let school management know if they decide to do this.)

NASUWT guidance states;

- To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly.

- Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your school.

As a minimum, NASUWT recommends the following:

Privacy Setting	Recommended security level
Send you messages	Friends only
See your friend list	Friends only
See your education and work	Friends only
See your current city and hometown	Friends only
See your likes, activities and other connections	Friends only
Your status, photos, and posts	Friends only
Bio and favourite quotations	Friends only
Family and relationships	Friends only
Photos and videos you're tagged in	Friends only
Religious and political views	Friends only
Birthday	Friends only
Permission to comment on your posts	Friends only
Places you check in to	Friends only
Contact information	Friends only

- Always make sure that you log out of Facebook after using it, particularly when using a machine that is shared with other colleagues/students. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure

you clear your chat history on Facebook (click "Clear Chat history" in the chat window).

- Employers may scour websites looking for information before a job interview. Take care to remove any content you would not want them to see.

Conduct on social networking sites:

- Do not make disparaging remarks about your employer/colleagues. Doing this in the presence of others may be deemed as bullying and/or harassment.
- Act in accordance with your employer's information technology (IT) policy and any specific guidance on the use of social networking sites. If your school/college encourages the positive use of social networking sites as part of the educational process, they should provide clear guidance on what is considered to be appropriate contact with students. Having a thorough policy in place will help staff and students to keep within reasonable boundaries
- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed. If you face disciplinary action as a result of being tagged, contact NASUWT immediately.
- Parents and students may access your profile and could, if they find the information and/or images it contains offensive, complain to your employer.
- If you have any concerns about information on your social networking site or if you are the victim of cyberbullying, you should contact your NASUWT Regional Centre immediately.
- Do not publish your date of birth and home address on Facebook. Identity theft is a crime on the rise with criminals using such information to access to your bank or credit card account.
- Be aware of what monitoring, if any, may be carried out by the school/college. Full details of this should be detailed in the IT policy.
- Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click "Privacy Settings". Under "Applications and websites" click "edit your settings". Scroll down to "instant personalisation" and make sure the checkbox for "enable instant personalisation on partner websites" is unchecked.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.

This guidance is applied through the Local Authority's policy on the agreed use of social networking sites and the school's acceptable use and E-Safety code of conduct. All staff and visitors including students have to sign these when they join our staff team (See Appendices 1 and 6)

3.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security. Video conferencing for pupils can only take place under the direct supervision of a member of staff for educational purposes. Examples may be conferencing with another school, or for some aspects of remote learning (additional information can be found in the Remote Learning Policy 2021).

- All software for webcam use will be password protected (Skype etc).

- Best practice recommends that schools always seek consent from parents for any video-conferencing. **See Appendix 8**

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and potential risks will be considered before use in school is allowed.

- Staff are allowed to have mobile devices in school but these must not be used during working hours except for school or emergency based communication in office areas, the staffroom and PPA room (see appendix 7)

- Pupils are not allowed mobile phones or mobile devices (such as iPods, games machines) with wireless Internet access that can bypass school filtering systems and present a new route to undesirable material and communications.

- Mobile phones and devices are to be handed in to either the class teacher or school office at the beginning of each school day. These will be returned to the student at the end of the school day.

- Personal mobile devices will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

- Staff will be issued with a school mobile phone where contact with pupils is required or school camera to capture photographs of pupils. Staff must not take photographs on their personal phones. Guidance @ Children, Families, Health and Education Directorate page 7 June 2008.
  See also our 'Mobile Phone Policy'.

3.9 Protecting and storing sensitive data including images

Personal data will be recorded, processed, transferred and made available according to data protection laws. This information will be clearly communicated to all staff, including office staff on an annual basis.

Staff are aware that they have a professional responsibility to ensure the following;

- All laptops must be password protected. Work laptops cannot be used for the storage of any inappropriate material.
- All data and images of children must be stored in the staff shared area on the curriculum network or the school's secure administration network.
- Photographs cannot be stored on personal laptops.
- No data or images can be transported out of the school without the device being approved or password protected.

3.10 Use of Photographs

Data protection affects our use of photography. This is because an image of a child is personal data for the purpose of GDPR and the Data Protection Act 2018 and it is a requirement that consent is obtained from the parent of a child or young person under the age of 18 years (or the child him or herself if deemed competent from 12 years old as suggested by the Information Commissioner) for any photographs or video recordings for purposes beyond the school's core educational function. (E.g. school web sites, school productions). At Heygarth Primary School we seek permission for all photography and video use.

There will also be times where the school will be carrying out off-site activities e.g. educational visits and residentials. Our guidelines are created to make sure that all images are taken appropriately by both adults in the school and children taking part in visits.

For both school setting and other events which are photographed for publicity purposes, additional consent should be sought from the child's parent/guardian of the child and kept on file, covering all cases where images of children are to be published beyond the parameters of school use.

Where children are 'Looked After' schools must check consent on the corporate parent's behalf with the social worker and there may be other situations, (in adoption placements or following a resettlement from domestic violence for example), where a child's security is known by the class teacher to be at stake, indicating the need for extra care.

Consent gained for photographs or videos may not extend to webcam use, so it is important to check, when introducing such technology, the status of existing consent for pupils or models.

Consent is sought for the whole time that children are at Heygarth Primary School. Parents retain the right to withdraw consent at any stage, but they need to do so in writing.

3.10a Planning photographs of children

Images and details of pupils published together allow for the remote possibility that people outside the school could identify and then attempt to contact pupils directly. The measures described below should help to minimise the risk of such unsolicited attention.

- Where possible, use general shots of classrooms or group activities rather than close up pictures of individual children.

- Use images of children in suitable dress, and take care photographing PE events to maintain modesty, using team tracksuits if appropriate for example. Photographs should not be taken of swimming pool-based events.

- Remember to include images of children from different ethnic backgrounds in your communications wherever possible, and positive images of children with disabilities to promote your school as an inclusive community, and to comply with the Disability Discrimination Act.

- Decide whether parents and visitors will be permitted to take photographs of the event. This must be authorised.

3.10b Identifying children

If the pupil is named, avoid using their photograph. If the photograph is used, avoid naming the pupil.

It is our policy that;

- You use the minimum information. Ask yourself whether it is really necessary to accompany a picture with the pupils' names, the year group, or the school.

- When *fully* naming pupils in any published text, whether in the school's brochure, website, or in the local press, avoid using their photograph, unless you have parental consent to do so.

3.10c Using photographs of children supplied by a third party

When using third parties, it is our school's responsibility to check that the adults are aware of the school protocols. In addition, we would expect that the adult taking the

images has a full DBS or is supervised when taking images by a member of the school's staff.

Children should never be left alone with a photographer.

Copyright does not apply to images for private family use. However, copyright does exist in commercial photographs and it rests with the photographer. Copyright is a right that the photographer automatically enjoys as the creator of the work to prevent other people exploiting his or her work and to control how other people use it. If you commission photographs for use at school/setting or work include in your contract that the school will own the copyright for items taken on your behalf.

3.10d Use of Images of children by the Press
(Please refer to the recommendations in section 3.10b above; 'Identifying Pupils')
There may be occasions where the press takes photographs at school of pupils. If this occurs we will ensure that specific permission is sought from the parent about whether to agree to their children being featured in the press and whether their full name should accompany the photograph.

3.10e Videos
School will ensure that parental consent is in place before any child can appear in a video. Parents can make video recordings of nativity plays and other such events for their own personal and family use, as they are not covered by the Data Protection Act. (Please refer to section 3.10h).

3.10f   Websites
Web use can be of particular concern to parents and staff because of the potential misuse of images by paedophiles. With digital photography there is the remote possibility that images of children could be produced, manipulated and circulated without the parents or children's knowledge. The dual concern which follows such a risk is that children might be exploited and a school or setting might be criticised or face legal action. Images on website can be made more difficult to copy by several measures - copy-protection, overlaying with a watermark, or published in low definition.

It is important to take care with identification and to respect parental views on the use of any photography of children on a website.

Increasingly adults and children are generating content for websites and applications e.g. children and adults placing pictures and/or videos on **Facebook, Instagram and TikTok**. It is therefore important that schools/organisations ensure that children, staff and parents understand the risks involved and are encouraged to adopt safe practice when generating content for school related websites.

This is included on our permission forms. Parents and staff are not allowed to share school images on any Internet sites or apps.

3.10h Parental right to take photographs and videos
We want parents to have the opportunity to record school events safely and responsibly.

We will allow recording, unless we feel that the images created may be inappropriate (for example a swimming gala). We also have to ensure that consent is gained for all children taking part.

Parents are not covered by data protection laws if they are taking photographs or making a video recording for **their own private use**. The Act does not, therefore, stop parents from taking photographs or making video recordings at school events, such as nativity plays or other such performances.

Parents are not permitted, however, to take photographs or to make a video recording for anything other than their own personal use (e.g. with a view to selling videos of a school event). Recording and/or photographing other than for private use would require the consent of the other parents whose children may be captured on film. Without this consent data protection laws would be breached.
See Appendix 9

3.10i Images **taken by young people**
Children do have permission to take photographs on days out and residential trips, etc. We will ensure that children understand that photographs must be responsible and not taken in private places, for example, in bedrooms or toilets.

3.10j Use of Mobile Phones
Children are not allowed to use mobile phones in school. We allow children to bring mobile phones to school must these must be locked in their class safe.

Staff are not allowed to video or take photographs of children using mobile phones as the data is not easily transferrable and may breach our obligations under the Data Protection Act.

Visitors are also informed of this as part of our safeguarding statement.

Parents can use them for recording only based on the guidelines above.

Please see also out 'Mobile Phone Policy'.

4.1 Authorising Internet access
- All staff must read and sign the 'Staff Code of Conduct for ICT' (see Appendix 1) before using any school ICT resource.

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

- All Parents/Guardians will be asked to sign and return a consent form.

- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' (see Appendix 5) before being allowed to access the internet from the school site. This includes governors, student teachers etc.

4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor LA can accept liability for any material accessed, or any consequences of Internet access.

- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)

- Pupils and parents will be informed of consequences for pupils misusing the Internet.

- Discussions will be held with the Police Youth Crime Officer to establish procedures for handling potentially illegal issues. Children, Families, Health and Education Directorate page 8 June 2008

4.4 Community use of the network and Internet

- Through extended schools use and partnership with other organisations there will be wider community use of the school's network. The school will liaise with local organisations to establish a common approach to e-safety.

- All consent forms must be used for these groups.

Communicating the E-Safety Policy

5.1 Introducing the e-safety policy to pupils
- E-Safety will be embedded in computing lessons and will incorporate materials from CEOP. Pupils in KS2 will also have access to the SAFE programme which is linked to Makewaves school safe social network site to develop skills, self-confidence and safety awareness in e-safety.

- E-Safety rules will be posted around school and discussed with pupils regularly as part of Computing lessons.

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

- E-Safety training will also come into the Personal Social and Health Education (PSHE) curriculum as well as the Digital Literacy strand of the Computing Curriculum.

5.2 Staff and the e-Safety policy
- All staff will be given the School e-Safety Policy and its importance explained.

- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

- Staff are encouraged to use a child friendly safe search engine when accessing the web with pupils.

5.3 Enlisting parents' and guardians' support

- Parents and guardian's attention will be drawn to the School e-Safety Policy on the school Web site.

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

This policy outlines acceptable use of the Internet and the Wirral Learning Grid.

All members of staff, pupils, students and all other users including Governors are required to follow all the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user's access to the school network and in some extreme instances of misuse could lead to criminal prosecution. In the case of employees, any breach may also be considered a breach of the employee's conditions of service, which could lead to dismissal on grounds of gross misconduct.
All users are expected to demonstrate a responsible approach to the use of resources available to them and to show consideration for other users both locally and with whom they may come into contact on the Internet.

Use of the Internet and facilities such as the electronic mail service are intended for educational purposes only. It must be recognised that any view communicated over the Internet is deemed to be a view of the school and in some circumstances the Council, akin to formal correspondence issued by post. Personal views about the school or Council business in an Internet communication should not be given or must be endorsed by the senior person in the school. No pupil should be identified directly by his or her email address. This will help to protect from unsolicited email.

The school's equipment and the Internet may only be used for legal activities consistent with the aims, objectives and rules of the school.

Unacceptable Deliberate Use
The following activities, whilst not an exhaustive list, are unacceptable:

1. The access to or creation, transmission or publication of any offensive, obscene or indecent images, sounds, data or other material.

2. The access to or creation, transmission or publication of any data capable of being displayed or converted to such obscene or indecent images, sounds, data or other material.

3. The creation, transmission or publication of any material which is designed or likely to cause offence, inconvenience or needless anxiety.

4. The creation, transmission or publication of defamatory material.

5. The receipt or transmission of material which infringes the copyright of another person or infringes the conditions of the GDPR or Data Protection Act 2018.

6. The transmission of unsolicited commercial or advertising material to other users of the Internet or any other network reachable via the Internet.

7. The deliberate unauthorised access to facilities, services, data or resources on any network or service accessible via the Internet.

8. Deliberate activities with any of the following characteristics or that by their nature would result in:
- Wasting staff or other users' efforts or network resources, either in school or elsewhere on the Internet and the efforts of staff involved in the support of those systems.
- Corrupting or destroying other users' data.
- Violating the privacy of other users (e.g. Data held on a network).
- Disrupting the work of other users whilst they are using the equipment in school.
- Using the Internet in a way that denies service to other users (for example, by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large files multimedia files).
- Continuing to use any item of software after being requested to cease its use because it is disrupting the correct functioning of the school's network or the Internet (for example, software designed to broadcast messages to all users of the Network).
- The deliberate introduction of "viruses" to the Network.

9. Where the Internet is being used to access another network, any abuse of that network will be regarded as unacceptable.

10. Any use of the Internet that would bring the name of the school or the Local Authority into disrepute.

11. The school's personal computers (including portables) must only be used to access the Internet through an officially authorised route.

12. The user should only print essential resource material and should always check the length of a document is reasonable before printing.

Each user (and in the case of pupils the parent, guardian or carer) is required to sign a document to acknowledge the stated conditions of use and advice given.

Declaration by Staff
All staff must sign to say they have read and understood read this policy document on use of the Internet and electronic mail and accept the stated conditions of use.

Review
This policy will be reviewed in line with the school's policy review programme. The subject leader is responsible for reporting to the governors about the quality of its implementation and its impact on standards. In the light of this, policy amendments may be made.

H. Beamish
September 2022