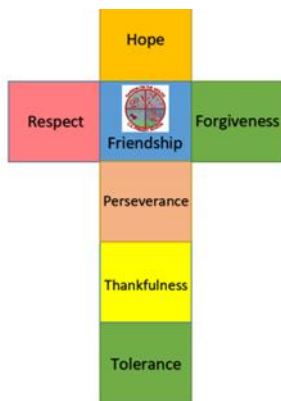


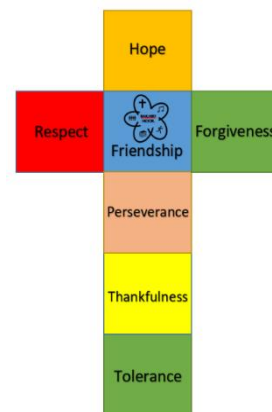
Barmby Moor and Garton on the Wolds CE Primary School



Respect, Aspire and Achieve

Our school works in partnership with the church and the wider community to give a caring and nurturing environment. Together we enable and equip everyone to have life to the full as Jesus promised. This vision is underpinned by the values of hope, friendship, respect, forgiveness, perseverance, tolerance and thankfulness.

"I have come that they may have life, and have it to the full" (John 10 v.10)



Barmby Moor and Garton on the Wolds and Barmby Moor CE Primary School

E-Safeguarding Policy

WHY IS INTERNET USE IMPORTANT?

The internet has become increasingly accessible for children and young people in places like schools, libraries and their own homes. Children and young people will experiment online to enable them to take advantage of the many educational and social benefits of new technologies learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviours.

- Children and young people use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students/children and young people who show a responsible and mature approach to its use.
- The purpose of Internet use in our school is to raise educational standards, to promote pupil/children and young people's achievement, to support the professional work of staff and to enhance the school's management functions.

HOW DOES INTERNET USE BENEFIT CHILDREN?

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet.

Benefits of using the Internet include:

- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- access to world-wide educational resources including museums and art galleries;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- exchange of curriculum and administration data with ERYC and DfE;
- access to learning wherever and whenever convenient.

HOW CAN WE ENSURE INTERNET USE ENHANCES LEARNING AND LIFE EXPERIENCES?

Children need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet.

Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- Internet access will be designed to enhance and extend education.
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Garton on the Wolds and Barmby Moor CE Primary School will ensure that the copying and subsequent use of Internet derived materials by staff and children complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of children.
- Staff should guide children to on-line activities that will support the learning outcomes planned for their age and maturity.
- Children and young people will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

HOW WILL CHILDREN LEARN HOW TO EVALUATE CONTENT?

Information received via the Internet, email or text message requires good information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

The extent to which the internet is used by extremists as a tool for radicalisation is not fully known but it is clear that persons responsible for recent attacks have accessed and been influenced by the internet to varying degrees. Extremist websites and social media access are used to disseminate propaganda, spread news and updates on extremist issues, add radical interpretation to theological tracts and provision of discussion forums for like minded individuals. The internet also offers easily accessible downloadable extremist material including advice and guidance on

bomb making, filtered out of public systems, but often not at home – policies need to empower children and young people to evaluate content critically.

- Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.

HOW WILL INFORMATION SYSTEMS SECURITY BE MAINTAINED?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff, children and young people. Data security is a complex matter and cannot be dealt with fully in this document. We see data security as the responsibility of all staff, e.g. maintain password security, care of equipment etc. Specifically the Headteacher, supported by the Senior Leadership team and the School Business Manager take a lead in this area. Please report any problems to the Headteacher. All staff with access to personal data are liable in law to protect that data. Should data be lost from an unencrypted USB drive or seen on a laptop used by other people, the consequences could be serious for the member of staff, for the school or organisation.

Local Area Network (LAN) security issues include:

- Access to all computing systems shall be via unique login and password. Any exceptions shall be recorded in the risk assessment and approved by the person in charge of data security.
- Where possible, all information storage shall be restricted to only necessary users. Access granted to new groups of users (for example, an external group attending a school-based event) shall be approved by the person in charge of data security. (The headteacher)
- All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) shall be authorised by the headteacher.
- Where 'restricted' information is stored, access shall only be granted to individuals approved by the headteacher. A record shall be kept of these approvals.
- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes that compromise access or security and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed and must be password protected.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils'/staff work areas or attached to email.
- Files held on the organisation's network will be regularly checked.
- The IT maintenance contractor will review system capacity regularly.

HOW WILL FILTERING BE MANAGED?

Levels of Internet access and supervision will vary according to the child or young person's age and experience. Access profiles must be appropriate for all members of the organisation.

- Our school uses East Riding of Yorkshire Council for Broadband provision and filtering systems.

- Requests for filtering changes from within the organisation will be made via the School Business Manager.
- The Headteacher and the School Business Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Google for Education will have access restrictions and usage monitored by the East Riding filtering systems.
- Any material that the organisation believes is illegal must be reported to the appropriate agencies such as Children's Social Care, IWF or CEOP.

HOW CAN EMERGING TECHNOLOGIES BE MANAGED?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, apps, collaboration, multimedia tools and social media. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom and/or organisational use. The safest approach is to deny access until a risk assessment has been completed and safety established. Virtual online classrooms and communities widen the geographical boundaries of learning. The safety and effectiveness of virtual communities depends on users being trusted and identifiable.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the organisation is allowed.
- Staff will be issued with the school's mobile phone during a residential visit where contact with parents is to be maintained in case of emergency.

HOW SHOULD PERSONAL DATA BE PROTECTED?

The quantity and variety of data held on children and young people, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

GDPR gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner Office, unless they are exempt.

GDPR applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards, which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

Data Protection Principles

All processing of personal data must be conducted in accordance with data protection principles. Our school policies and procedures are designed to ensure compliance with these principles, which are set out fully in our Data Protection Policy:

- Personal data must be processed lawfully, fairly and transparently

- Personal data can only be collected for specific, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to what is necessary for processing
- Personal data must be accurate and kept up to date with every effort to erase or rectify without delay
- Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
- Personal data must be processed in a manner that ensures the appropriate security
- The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

Data protection legislation includes provisions that promote accountability and governance. These complement the transparency requirements. This accountability additional principle requires the school to demonstrate that it complies with the principles and states explicitly that this is the school's responsibility.

Our school demonstrates this compliance through our Data Protection policy, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, and establishing formal procedures in relation to data protection.

Organisations will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

PASSWORD SECURITY

Staff are provided with Encrypted pen drives to ensure data protection.

Members of staff/volunteers with access to computing systems shall be responsible for taking the appropriate steps to select and secure their passwords. These steps should include:

- Keeping their password secure from others.
- Using a different password for accessing organisational systems to that used for personal (non-organisational) purposes.
- Choosing a password that is difficult to guess, or difficult for others to obtain by watching them login.
- Adding numbers or special characters (e.g. !@£\$%^) can help.

HOW WILL EMAIL BE MANAGED?

The implications of email use by children and young people needs to be thought through and appropriate safety measures put in place. Un-regulated email can provide routes to children and young people that bypass the traditional boundaries.

A central question is the degree of responsibility that can be delegated to individual children and young people, as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible.

The use of email identities such as john.smith@[school] generally needs to be avoided by children and young people, as revealing this information could potentially expose a child to identification by unsuitable people.

Children will not be allowed access to send and receive emails from the Google for Education account.

For primary schools, whole-class or project email addresses may be used.

- Children may only use approved email accounts.
- Children must immediately tell an adult if they receive offensive email.
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

HOW WILL PUBLISHED CONTENT BE MANAGED?

Excellent websites can inspire children and young people to publish work of a high standard. Websites can celebrate children and young people's work, promote our school and publish resources for projects. Sensitive information about the school and children could be found in a newsletter but the website is more widely available. Publication of information should be considered from a personal and school security viewpoint.

- The contact details on the website should be the school's name, address, email and telephone number. Employee/volunteer or children's personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. consider replacing '@' with 'AT').
- The appointed senior leader will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with guidelines for publications including respect for intellectual property rights and copyright.

CAN PUPIL IMAGES AND WORK BE PUBLISHED?

Although common in online sources, including newspapers online, the publishing of children names with their images is not acceptable.

Strategies include using relatively small images of groups of children and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the organisational activity. Personal photographs can be replaced with self-portraits or images of children and young people's work or of a team activity. Children in photographs should, of course, be appropriately clothed.

Images of children should not be published without the parent's or carer's written permission. Some organisations ask permission to publish images of work or appropriate personal photographs on entry, some once per year, others at the time of use.

Children also need to be taught the reasons for caution in publishing personal information and images online.

- Images that include children will be selected carefully and will not provide material that could be reused.
- Children's full names will not be used anywhere on the website or social media, particularly in association with photographs.

- Written permission from parents or carers will be obtained before images of children are electronically published. Parents are asked to sign a permission slip on entry to the school, staff should check for exclusions in their class.

HOW WILL SOCIAL NETWORKING AND PERSONAL PUBLISHING BE MANAGED?

Parents/carers and professionals need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.

Children should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All adults should be made aware of the potential risks of using social networking sites or personal publishing either professionally with children and young people or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. The internet and social networking sites may provide a virtual online community to which a young person may wish to belong and then may in turn become increasingly exposed to extremism. Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others.

- Barmby Moor and Garton on the Wolds CE Primary School will control access to social media and social networking sites during the school day and children and staff will be advised on their use and associated dangers out of school.
- Children will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, Instant Messaging and email addresses, full names of friends/family, specific interests and clubs etc.
- Children should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the child or young person or his/her location.
- Employee/volunteer official blogs or wikis should be password protected and run from the organisational website with approval from the Senior Leadership Team/Senior Manager.
- Employee/volunteer should be advised not to run social network spaces for children and young people's use on a personal basis.
- Children should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children should be encouraged to invite known friends only and deny access to others by making profiles private.
- Children are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Children are now exposed to a plethora of social media sites. The children at our school are too young to use such sites as they are age restricted. Class teachers will talk about issues as they arise and as they are appropriate. Any incidents related to social networking sites will be logged in the office and will be acted upon.

HOW WILL INTERNET ACCESS BE AUTHORISED?

Our school will allocate Internet access for staff members/volunteers, children and young people on the basis of educational need

Pupil usage will be fully supervised.

Parental permission shall be required for Internet access in all cases.

- Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- The Acceptable Use Policy is discussed in classes as an age appropriate document.

HOW WILL RISKS BE ASSESSED?

E-security and e-safety is based upon the assessment of risk, and the implementation of controls to manage these risks; no use of digital technology is completely risk free. Information security is critical, in both protecting the information held concerning staff/volunteers, children and young people, and in ensuring the reliability of computing systems to support teaching and learning.

- Our school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer. Neither Garton on the Wolds or Barmby Moor CE Primary School nor ERYC can accept liability for the material accessed, or any consequences resulting from Internet use.
- Our school will audit digital technological use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

HOW WILL COMPLAINTS BE HANDLED?

Parents, staff, children should know how to use the organisation's complaints procedure. Potential child protection and illegal issues must be referred to the organisation's Designated Safeguarding Lead or Deputy Safeguarding Lead and/or E-safety Co-ordinator. Please refer to the Response to Risk Flowchart for reporting e-safety incidents.

- Complaints of Internet misuse will be dealt with under Complaints Procedure.
- Any complaint about staff misuse must be referred to the E-safety Co-ordinator.
- All e-safety complaints and incidents will be recorded by the school — including any actions taken using a log held centrally in the office.
- Children and parents/carers will be informed of the complaint's procedure. Children will be talked to in a child friendly way.
- Parents/carers, children will work in partnership with the school to resolve issues.
- Any issues (including sanctions) will be dealt with according to our school's disciplinary and child protection procedures.

HOW WILL CYBERBULLYING BE MANAGED?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" (DCSF 2007).

It is essential that children, young people, organisations, and parents/carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

- Cyberbullying (along with all forms of bullying) will not be tolerated at our school. Full details are set out in our policy on anti-bullying.
- There will be clear procedures in place to support anyone affected by cyberbullying. The child/parent should inform the class teacher/head teacher. The head teacher will investigate, see interested parties and take appropriate action in line with the bullying policy.
- All incidents of cyberbullying reported will be recorded and are kept in the School Office in the E-Safeguarding Incident Log.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying: Children, staff/volunteers and parents/carers will be advised to keep a record of the bullying as evidence.

Our school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended for the user for a period of time.
- Parents/carers may be informed.
- The Police will be contacted if a criminal offence is suspected.

RESPONSE TO AN INCIDENT OF CONCERN

An important element of e-safeguarding is the ability to identify and deal with incidents of concern and related to the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report e-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The organisation shall establish an incident reporting procedure and record reported incidents on the child's log.

The Incident Log shall be formally reviewed, and any outstanding actions delegated, by the Senior Leadership Team/senior manager within the organisation at a minimum frequency of once per term. Through this review process, where deemed appropriate, management shall update the risk assessment in light of new incidents. The Log and accompanying action plans should be reviewed annually by the Governing Body.

Organisations could usefully draw up a list of common incidents from the log. For example:

- * Circumventing the network security system
- * Accessing inappropriate material
- * Installing unapproved software
- * Using other people's accounts, email addresses or passwords
- * Breaching copyright

- * Uploading school material onto a social network or chat room
- * Leaving school mobile devices unattended
- * Not logging off when leaving a device
- * Child Exploitation and Online Protection (CEOP)

Children need to know how to block someone online and report them if they feel uncomfortable. It is important to realise that there are people other than the staff in your organisation who can help. Online child abuse can be reported directly, as well as requests to seek out more advice and support.

Reports can be made directly to CEOP through their Click CEOP reporting button, which is present on an increasing number of websites and social networks.

WHAT SHOULD THE COMMUNICATIONS PLAN CONTAIN?

Our school shall include appropriate communications and/or training for all sectors of the organisation's community.

This should cover:

- Workforce training in understanding the rationale for all e-safeguarding procedures and the consequences of inappropriate practice.
- Workforce training in responsible approaches to data on mobile devices, communicating online and procedures when using multimedia digital content such as photographs, videos and podcasts in terms of permission seeking, taking, storage and retention.
- A comprehensive and developmental e-safety curriculum for children and young people referenced in schemes of work and programmes of study in schools.
- The programme should include the responsible use of web and communication technologies both inside and outside school and risks related to cyberbullying.
- Regularly re-visiting of the AUP with staff and pupils.
- ICT non-teaching staff training related to how digital technology can enhance learning and teaching.
- Organisations shall create working Acceptable Use Policies (AUPs) based on all the agreed procedures for e-security and e-safety and covering ICT usage by all sectors of the organisational community. This policy shall be subject to annual review by the governing body.

Organisations like ChildNet, ThinkyouKnow, CEOP offer support for education and training materials.

The children and parent agreement will be sent out to all parents. The policy will be on the web site and reminders will be put in newsletters. Consideration must be given as to the curriculum place for teaching e-safety; it could be as a computing lesson activity, part of the pastoral programme or part of every subject whenever children and young people are using the internet.

All staff including administration, governors and volunteers shall be included in awareness raising and training. Induction of new staff/volunteers shall include a discussion of the organisation's e-safety Policy.

- The e-safety Policy will be formally provided to and discussed with all members of staff.

- To protect all staff and children, the organisation will implement Acceptable Use Policies.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor computing use will be supervised by the Senior Manager/ Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

Parent's support

- Parents'/carers' attention will be drawn to our e-safety Policy in newsletters and on our website as well as through the organisation's Child Protection Policy and Procedures.
- A partnership approach with parents/carers will be encouraged.
- Parents/carers will be requested to sign an e-safety/internet agreement as part of the Home School Agreement.
- Information and guidance for parents/carers on e-safety will be made available to parents/carers in a variety of formats.

REVIEW

This policy will be reviewed in the Spring 2021 or earlier if deemed necessary.

Signed Governor

Signed Headteacher

Date

Rules for Responsible Internet Use

PUPILS (provided in Admission Pack and Prospectus)

RULES FOR RESPONSIBLE INTERNET USE

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others:

- I will ask permission from a member of staff before using the Internet.
- I will use only my own login and password, which I will keep secret.
- I will not access other people's files.
- I will use the computers only for schoolwork and homework.
- I will not bring any removable media (for example, CD's, memory sticks) into school unless I have permission.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I will not give my home address or phone number, or arrange to meet someone, unless my parent, teacher or carer has given permission.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

Rules for Responsible Internet Use

PARENTS (provided in Admission Pack and Prospectus)

RESPONSIBLE USE OF THE INTERNET

As part of pupils' curriculum enhancement and the development of ICT skills, Barmby Moor & Garton on the Wolds Schools are providing supervised access to the internet including email and a safe school monitored version of social media.

Our school internet access provider and Google for Education administrator operates a filtering system that restricts access to inappropriate materials.

Photographs taken in school should remain personal property and not shared on personal social media accounts. This is in consideration of safeguarding in school.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school nor the LA cannot be held responsible for the nature or content of materials accessed through the Internet. The School and the LA will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

A copy of the Rules for Responsible Internet Use that we operate at Barmby Moor & Garton on the Wolds Schools is provided.

Should you wish to discuss any aspect of Internet use please telephone the school office to arrange an appointment.

- Correlating with Children's Online Privacy Protection Act (COPPA) guidelines children will not have their own social media accounts such as Facebook, Snapchat, Whatsapp and others throughout their time at Barmby Moor & Garton on the Wolds Primary Schools. If these accounts are created, as a parent or guardian, I understand that it is my responsibility for the account and monitoring the account.
- For information a list of sites and the required age for use is attached.

Permission for Internet Access	
Parent/Carer's Permission	Pupil's Agreement
I give permission for access to the Internet on the terms set out above.	I agree to follow the Rules for Responsible Internet Use.
Signed:	Signed:
Print name:	Print name:
Date:	Date:

Age Restrictions for Social Media Sites

The minimum age restricts for social media sites are as follows:

Age 18 (or 13 with parent's permission):

YouTube

Flickr

Keek

Age 16:

Whatsapp

Age 13:

Twitter

Facebook

Snapchat

Instagram

Reddit

Tumblr

Goggle+

Pinterest

Parents should also be aware of other more prevalent social media accounts such as: Musical.ly and Clash of Clans etc.