BRUNSWICK INFANT SCHOOL

e-SAFETY POLICY

2021 / 2022

Mrs S Waugh
Acting Head teacher

Sam Waugh

Signed:
Date: 8th November 2021

Pierre Crubilier
Chair of Governors

Pierre Crubilier

Signed:
8th November 2021

This policy will be reviewed annually

Due for review: December 2022

Contents

Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students/pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school e-Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students/pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student/pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing/distribution of personal information / images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyberbullying;
- Access to unsuitable video/internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-Safety policy is used in conjunction with other school policies including the overarching Safeguarding Policy, GDPR and Data Protections Policies Statement, and Whole School Behaviour Policies for example – see Point 1 below.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students'/pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1. Associated School Policies

This Policy should be read in conjunction with the following school policies/procedures:

- Overarching Safeguarding Policy incorporating Child Protection
- GDPR
- Data Protection Policy
- Health and Safety Policy
- Procedures for Using Pupils Images
- Whole School Behaviour Policy

X:\policies\health&safety safeguarding\e safety

- Cumbria County Council Information Technology Acceptable Use Guidance for School Based Staff

2. Development/Monitoring/Review of this Policy

This e-Safety policy has been developed by the e-safety working group made up of: Pierre Crubilier, Sharon Sanderson with advice from Jeff Haslam. All the following groups will be consulted:

- *School e-Safety Coordinator*
- *Head teacher/Senior Leaders*
- *Teachers*
- *Support Staff*
- *ICT Technical staff*
- *Governors*
- *Parents and Carers*
- *Community users – to be reviewed as appropriate.*

Consultation and communication with the whole school community has taken place through the following:

- *Staff meetings*
- *Governors meeting/ policy group sub-committee meeting*
- *Parents questioners and parent governor involvement in working group*
- *School website/newsletters/advice documents for staff, pupils and parents.*
- *1 to 1 conversations with parents.*
- *Reminders at school events such as church services / performances*

2.1 Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the *Governing Body/Governors Sub-Committee on:*	*Insert date: first approved on 18th Dec 2012 and reviewed annually.* *Revision April 2019*
The implementation of this e-Safety policy will be monitored by the:	*e-safety working group and the governors policy group.*
Monitoring will take place at regular intervals:	*Annual monitoring by policy group.* *On going monitoring by the e-safety coordinator. This would include visits to classrooms and conversations with staff and pupils.*
The *Governing Body/Governors Sub-Committee* 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 by the e-safety coordinator*
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:	*Six months after the initial implementation and 12months thereafter.*
Should serious e-Safety incidents take place, the following external persons/agencies should be informed:	*LADO - LSCB* *Police* GDPR breach guidelines to be followed (see school policy guidelines)

The school will monitor the impact of the policy using:

- *Logs of reported incidents in green file*
- *Kidsafe programme in Y2*

- *Annual information to parents with reply slips.*

3. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers, 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. This is pertinent to incidents of cyberbullying, or other e-Safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and the Whole School Behaviour Policy which includes anti-bullying and will, where known, inform parents/carers of incidents of inappropriate e-Safety behaviour that take place out of school.

GDPR breaches will be reported in line with the school policy

4. Roles and Responsibilities

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

4.1 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 chair of governors in his role as e-safety coordinator. He will be supported by the e-safety working party including a parent governor and headteacher. The governing body sub-group for policies will take responsibility for ensuring the policy is reviewed. An annual report will be provided by the e-safety governor on the implementation and monitoring of the policy at the AGM.
The role of the e-Safety Governor / coordinator will include:

- *regular monitoring of e-Safety incident logs*
- *reporting to relevant Governors committee/meeting*

4.2 Head teacher and Senior Leaders

- The Head teacher is responsible for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety will be delegated to the e-Safety Co-ordinator. However, all staff would be expected to have a shared responsibility.
- The Head teacher is responsible for ensuring that the e-Safety Coordinator and relevant staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The Headteacher and Governors will receive regular monitoring reports from the e-Safety Coordinator.
- The Head teacher and the Assistant Head 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 (see flow chart on dealing with e-Safety incidents – Appendix F, and relevant Local Authority HR/school disciplinary procedures). The procedures for dealing with allegations against staff can be found within the school Safeguarding Policy.

4.3 e-Safety Coordinator

- 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;
- facilitates training and advice for staff;
- liaises with the Local Authority (where appropriate);
- liaises with school's ICT technical support staff;
- receives reports of e-Safety incidents and creates a log (green file) of incidents to inform future e-Safety developments;
- meets regularly with e-Safety working party to discuss current issues, review incident logs and any other relevant issues.
- attends relevant meeting/committee of Governors;
- reports regularly to School Staff.

4.4 Network Manager/Technical staff

The Network Manager/Systems Manager/ICT Technician/ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets the e-Safety technical requirements outlined in the School e-safety / Acceptable Use Policy and any relevant Local Authority e-Safety Policy and guidance;
- that users may only access the school's networks through a properly enforced password protection policy, in which staff are encouraged to change their passwords regularly;
- *the school's filter is provided by the broadband provider and is regularly monitored for effectiveness.*
- that he/she keeps 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/website /remote access/email* is regularly monitored in order that any misuse/attempted misuse can be reported to the *Head teacher for investigation/action/sanction.*

4.5 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/Agreement (AUP) – see Appendix D.
- they report any suspected misuse or problem to the e-Safety Co-ordinator and or Head teacher for investigation.
- digital communications with pupils should be on a professional level and only carried out using official school systems.
- e-Safety is embedded in all aspects of the curriculum and other school activities.
- pupils understand and follow the school e-Safety and acceptable use policy/Agreement – see Appendix B;
- they monitor ICT activity in lessons, extra-curricular and extended school activities;
- they are aware of e-Safety issues related to the use of mobile phones, cameras and hand held 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.
- Staff are aware of GDPR regulations and school policy on sharing/storing information and images

4.6 Designated Person for Child Protection (DPCP)

Should be trained in e-Safety issues and be aware of the potential for serious child protection issues to arise from:

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

4.7 e-Safety Working Party

Members of the e-Safety working party will assist the e-Safety Coordinator with the production/review/monitoring of the school e-Safety policy/documents;

4.8 Pupils

Taking into account the age and level of understanding of our young pupils:

- Will be guided in using the school ICT systems in accordance with the Pupil Acceptable Use Policy/Agreement and Think then Click guidelines – see Appendix B & C, which their parents/carers will be expected to sign before being given access to the internet;
- Need to understand the importance of reporting inappropriate content.
- Should know the importance of adopting good e-safety practices at home.
- Year 2 pupils have e-safety training through Kidsafe programme.

4.9 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through information guidance on e-safety. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy/Agreement (AUPA) – see Appendix B;
- Ensuring that they themselves do not use the internet/social network sites/other forms of technical communication in an inappropriate or defamatory way.
- Following school guidelines on sharing information/images.

4.10 Community Users

Community Users who access school ICT systems/website as part of the Extended School provision will be expected to sign a AUP before being provided with access to school systems – see Appendix D.

5. Teaching and Learning

5.1 Why Internet use is Important

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education.
- The school has a duty to provide pupils with safe Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to question information from the internet and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

5.2 How Internet Use Benefits Education

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network (NEN) which connects all UK schools
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- 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;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DfE;
- access to learning wherever and whenever convenient.

5.3 How Internet Use Enhances Learning

- The school's Internet access will be used to enhance and extend pupils' independent learning.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

5.4 How Pupils will Learn How to Evaluate Internet Content

- Pupils will be taught to be critically aware of the materials they read and shown how to check the accuracy of information. (advise use several sources of information)
- Pupils will use age-appropriate tools to research Internet content.

5.5 Pupils with Additional Needs

At Brunswick School we strive to meet the needs of every child and take into account that some of our pupils may require extra support or a personalised plan to ensure they are given appropriate access to e-safety information.

- A fundamental part of teaching e-Safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.
- It might be helpful to consider presenting the rules as being linked to consequences such that you are teaching cause-effect rather than a list of procedures. This needs to be achieved carefully so as to use realistic and practical examples of what might happen if… **without frightening pupils**.

6. Managing Information Systems

6.1 Maintaining Information Systems Security

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked and GDPR guidance followed

- The ICT coordinator/network manager will review system capacity regularly.
- Use of user logins and passwords to access the school network will be enforced – see Section 6.2 below.

The school broadband and online suppliers are Talk Straight.

6.2 Password Security

The school will be responsible for ensuring that the school infrastructure/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, without permission (or as 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;
- logs are maintained of access by users and of their actions while users of the system.

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems including email).

The management of password security will be the responsibility of (network manager)

Responsibilities:

All staff 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.

Any changes carried out must be notified to the member of staff responsible for issuing and co-ordinating password security.

Users will change their passwords every 6 months (January and July)

Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss.
Members of staff will be made aware of the school's password security procedures:

- at induction;
- through the school's e-Safety policy;
- through the Acceptable Use Agreement;
- staff meeting updates

Students will be made aware of the school's password security procedures.

Policy Statements:

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager.

Audit/Monitoring/Reporting/Review:

The network manager will ensure that full records are kept of:

- User Ids and requests for password changes;
- User log-ons;
- Security incidents related to this policy.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner (safe).

6.3 Managing Email

Currently pupils do not use email accounts.
However, should school or government policy change the following guidelines will be followed:

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Headteacher.
- Access in school to external personal email accounts is not allowed.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of messages is not permitted without permission of originator.
- Staff should not use personal email accounts for sending sensitive school information.
- The official school email service may be regarded as safe and secure and is logged.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Spam, phishing and virus attachments can make email dangerous. The school ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

6.4 Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible;
- The use of Hotmail, BTInternet, AOL, Yahoo, Gmail or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted;
- Where your conclusion is that e-mail must be used to transmit such data:

- Use the headteacher Egress account for serious/sensitive information
  - Obtain express consent from your manager to provide the information by e-mail;
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail;
  - Verify the details, including accurate e-mail address, of any intended recipient of the information;

  - Verify (by phoning) the details of a requestor before responding to e-mail requests for information;
  - Do not copy or forward the e-mail to anyone without consent.

- Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
- Send the information as an encrypted document **attached** to an e-mail;
- Provide the encryption key or password by a **separate** contact with the recipient(s);
- Do not identify such information in the subject line of any e-mail;
- Request confirmation of safe receipt.

6.5 Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left;

6.6 Managing Published Content

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

6.7 Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, students/pupils and parents/carers need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 and parents should be aware of 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 e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs / videos of pupils are used.
- Pupil's work can only be published with the permission of the student/pupil and parents or carers.
- Images will not be stored for longer than the pupils attend the school

6.8 Managing Social Networking, Social Media and Personal Publishing Sites

- The school have a social media page (formerly k/a Facebook) which is updated by the Head and school staff and monitored by the Head and Governors.
- The school will control access to social media and social networking sites.

- Pupils 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, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Personal publishing and on-line communication will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding pupils' 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 students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and outlined in the school Staff/Governor/Student (trainee) Acceptable Use Policy – see Appendix D.
- Further guidance can be found in the Appendix - 'Online Communication Code of Conduct for Staff Working with Children' and the 'Safe Use of Facebook and Other Social Networking Sites'.
- A sample advice leaflet for parents on Social Networking Sites, in particular, Facebook, can be found at Appendix E.
- Parents are not allowed to put images or videos of school events/pupils on social media or send via internet.

6.9 Managing Filtering

- The school's broadband access will include filtering.
- The school will work with the Schools Broadband team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- The e-safety coordinator will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Cumbria Police or CEOP.

6.10 Managing Videoconferencing

- The school use Zoom and Teams software for online video conferencing and meetings with parents and other professionals. During periods on lockdown or class closures, Zoom can be used to facilitate assembly and online teaching and learning. A safe use procedure is shared with families and adult supervision is mandatory.

6.11 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

6.12 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.

More detailed information can be found in the School Data Protection Policy and GDPR Privacy statement.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Do not store personal data/images of past pupils.
- Historical log books and school diaries have been given to Cumbria Archive Service.

6.13 Disposal of Redundant ICT Equipment

Any redundant PCs will have hard drives destroyed.

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to:
  - The Waste Electrical and Electronic Equipment Regulations 2006
  - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  - Environment Agency Guidance (WEEE)
  - ICO Guidance - Data Protection Act 1998
  - Electricity at Work Regulations 1989
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The school's disposal record will include:
  - Date item disposed of;
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
  - How it was disposed of e.g. waste, gift, sale
  - Name of person and/or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times or 'scrubbed' to ensure the data is irretrievably destroyed.

6.14 Use of School I-pad and Linx tablets

The I-pads and tablets should only be use for school work, either at school, at home or on school trip.

The I-pads and tablets are protected by a password, **do not disclose the password to anyone not employed by the school and do not allow anyone not employed by the school to have access to any confidential data stored on or accessible through the I-pad or tablet**

If you forgot your password ask the Headteacher or Business Support Lead to issue you a new password. The I-pads are set to erase all data after unsuccessful attempt at login.

The I-pads and tablets are not be used to access any personal social media, i.e. Facebook, FaceTime etc.

Please make sure that you have logged off ScholarPack at the end of each session, in particular if you are accessing the programme away from school.

7. Policy Decisions

7.1 Authorising Internet Access

- All staff will read and sign the Staff/Governor/Student (trainee) Acceptable Use Policy (Appendix D) before using any school ICT resources.
- Parents will be asked to read and sign the School Acceptable Use Policy for pupil access (Appendix B) and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign the Staff/Governor/Student (trainee) Acceptable Use Policy n Acceptable Use Policy (Appendix D).
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

According to Setting Type:

- Pupils' access to the Internet will be by adult demonstration and teacher directed independent work using specific and approved online materials.

7.2 Assessing Risks

- The 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 school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–safety policy is appropriate – see Appendix A for a sample e-Safety Audit.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Cumbria Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

7.3 Prevent Duty

- The School will play its role in equipping children to stay safe online, both in school and outside.
- Children are to be kept safe from terrorist and extremist material when accessing the internet in schools
- The School has ensured that suitable filtering is place

7.4 Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	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				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)			✓			
On-line gaming (non-educational)			✓			
On-line gambling					✓	
On-line shopping/commerce				✓		
File sharing					✓	
Use of social networking sites				✓		
Use of video broadcasting e.g. Youtube				✓		

7.5 What are the risks?

The risks that can be posed to young people and adults when online have been identified by the EUKids online project, which was later referenced in paragraph 1.3 of Dr Tanya Byron in "Safer Children in a Digital World" (2008).

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias, Racist or Misleading info or advice
Contact (Child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers, Being groomed	Self-harm, Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information/advice

Byron Review (2008)

7.6 Responding to Incidents of Concern

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

School should refer to the Flow Chart found at Appendix F.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Person for Child Protection will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Safeguarding Policy for dealing with concerns.
- The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Children's Services and escalate the concern to the Police.
- Any racist incidents will be reported to Children's Services. Racist Incident Monitoring forms should be completed electronically through the School Portal. This allows for individual incidents to be reported as and when they happen and will also generate a termly report for schools to agree to and return.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Local Authority Designated Officer (LADO) – see Safeguarding Policy.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

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

Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher/tutor	Refer to Head of Department/Head of Year/other	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).			✓	✓	✓	✓	✓		
Unauthorised use of non-educational sites during lessons	✓		✓		✓	✓			
Unauthorised use of mobile phone / digital camera / other handheld device	✓		✓		✓	✓			
Unauthorised use of social networking / instant messaging / personal email	Should not happen don't use social network sites / email with pupils. If this happens refer to head and e-safety coordinator for investigation before further action is taken.								
Unauthorised downloading or uploading of files	✓		✓	✓	✓	✓	✓		✓
Allowing others to access school network by sharing username and passwords	Not applicable								
Attempting to access or accessing the school network, using another student's/pupil's account	Not applicable								
Attempting to access or accessing the school network, using the account of a member of staff			✓	✓	✓	✓	✓		
Corrupting or destroying the data of other users	✓		✓	✓	✓	✓	✓		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓		✓	✓	✓	✓	✓		
Continued infringements of the above, following previous warnings or sanctions	✓		✓	✓	✓	✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓		✓	✓	✓	✓	✓		
Using proxy sites or other means to subvert the school's filtering system	Not applicable								
Accidentally accessing offensive or pornographic material and failing to report the incident	✓		✓		✓	✓		✓	
Deliberately accessing or trying to access offensive or pornographic material	✓		✓	✓	✓	✓			✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	Not applicable								

Staff	**Actions / Sanctions**							
Incidents:	Refer to line manager	Refer to Head teacher	Refer to LA/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓			✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓			✓	✓		
Unauthorised downloading or uploading of files		✓	✓	✓	✓	✓	✓	✓
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		✓			✓	✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓			✓	✓		
Deliberate actions to breach data protection or network security rules		✓	✓	✓	✓	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓	✓	✓			✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓	✓			✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✓	✓		✓	✓	✓	✓
Actions which could compromise the staff member's professional standing		✓			✓	✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓		✓	✓		
Using proxy sites or other means to subvert the school's filtering system		✓			✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓	✓		
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓	✓		✓	✓
Breaching copyright or licensing regulations		✓	✓	✓	✓	✓		
Continued infringements of the above, following previous warnings or sanctions		✓	✓	✓	✓			✓

7.7 Handling e–safety Complaints

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–safety complaints and incidents will be recorded by the school, including any actions taken (see Appendix I).
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police and/or Children's Services to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

7.8 How the Internet is used across the Community

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for pupils who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

7.9 Managing Cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- 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 if the bully refuses or is unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the Whole School Behaviour Policy, Acceptable Use Policy and Disciplinary Procedures.
  - Parent/carers of pupils will be informed.
  - The Police will be contacted if a criminal offence is suspected.

7.10 Managing Learning Environment/Platforms

- The school uses Discovery Education, Mathletics and Mathseeds to set online learning. The children have individual log ins and passwords for each and is monitored by the Chair of Governors.

7.11 Managing Mobile Phones and Personal Devices

- The use of mobile phones and other personal devices by staff and students in school will be decided by the school and covered in the school Acceptable Use Policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- Pupils are not allowed to use phones at school and are discouraged from bringing them onto the school site. If a pupil does bring a phone to school it will be kept safe by the school office until the end of the school day when parents / carers can collect it.
- Staff and student mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off or left on silent in the staffroom lockers or school offices.
- In the case of an emergency, permission can be sought from the headteacher to keep a mobile phone close at hand.
- The Bluetooth function of a mobile phone should not be used to send school images or school files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils use of personal devices:

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff use of personal devices:

- Staff are not usually permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. In exceptional circumstances, with permission by the Headteacher, personal devices may be used but personal numbers withheld by prefixing 141 before the number.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required (if available).
- Mobile phones and devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by Headteacher in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Due to COVID-19, staff may use personal devices to communicate if movement around the building must be restricted due to infection rates.

	Staff, students & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones or other camera devices	Allowed on school equipment only.						✓	
Use of hand held devices e.g. PDAs, PSPs							✓	
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of chat rooms/facilities		✓						✓
Use of instant messaging		✓						✓
Use of social networking sites		✓						✓
Use of blogs		✓						✓

8. Communication Policy

8.1 Introducing the Policy to Pupils?

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com

- Reminders at every school event, show and performance.
- All users will be informed that network and Internet use will be monitored.
- An e–safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e–safety module will be included in the school curriculum and reinforced throughout the year.
- e–safety will be part of the transition programme when moving between establishments.
- e-Safety rules will be posted in all rooms with Internet access – see Appendix C.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

8.2 Discussing the Policy with Staff

- The e–safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- 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. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

8.3 Enlisting Parents' Support

- Parents' attention will be drawn to the school e–safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged.
- Parents will be encouraged to read and sign the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

9. Acknowledgements

With thanks to Jeff Haslam (e-Safety Consultant), Hertfordshire County Council, Kent County Council, the South West Grid for Learning, Cumbria LSCB, CEOP, UKCCIS, Childnet and the DfE whose guidance and information has contributed to the development of this Policy.

SCHOOL e-SAFETY AUDIT APPENDIX A

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-Safety policy. Staff that could contribute to the audit include: Designated Person for Child Protection, SENCO, e-Safety Coordinator, Network Manager and Head teacher.

Does the school have an e-Safety Policy		**YES**
Date of latest update:	April 2019	
Date of future review:	April 2020	
The school e-Safety policy was agreed by governors on:	18th Dec 2012 and last agreed April 2019	
The policy is available for staff to access at:	Shared Documents -Policies	
The policy is available for parents/carers to access at:	Website	
The responsible member of the Senior Leadership Team is:	Sam Waugh – Acting Head Teacher	
The governor responsible for e-Safety are:	Pierre Crubilier & (vacancy)	
The Designated Person for Child Protection is:	Sam Waugh – Acting Head Teacher	
The e-Safety Coordinator is:	Pierre Crubilier	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?		**YES**
Has up-to-date e-Safety training been provided for all members of staff? (not just teaching staff)		**YES**
Do all members of staff sign an Acceptable Use Policy- this should happen at induction?		**YES**
Are all staff made aware of the schools expectation around safe and professional online behaviour?		**YES**
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?		**YES**
Have e-Safety materials from CEOP, Childnet and UKCCIS etc. been obtained?		**YES**
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?		**YES**
Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?		**YES**
Do parents/carers sign an Acceptable Use Policy?		**YES**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?		**YES**
Has an ICT security audit been initiated by SLT?		**YES**
Is personal data collected, stored and used according to the principles of the Data Protection Act?		**YES**
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?		**YES**
Has the school filtering been designed to reflect educational objectives and been approved by SLT?		**YES**
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?		**YES**
Does the school log and record all e-Safety incidents, including any action taken?		**YES**
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?		**YES**

APPENDIX B

PUPIL ACCEPTABLE USE POLICY / AGREEMENT

Brunswick Infant School

These rules will help us to be fair to others and keep everyone safe.

- I will only use ICT in school for school purposes.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will click on the Big Red Button and tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. When using the internet at school or at home. I will not arrange to meet someone unless my parents have agreed.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- Myself and my family will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community, including any images or videos from school assemblies, show or events.
- I will not share my login information for online learning platforms such as Mathletics and Mathseeds with anyone else.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

✂----------

Pupil Acceptable Use - Parent/Carer Agreement

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact **Mrs Waugh.**

Parent/Carer signature

We have discussed this and …… (child name) agrees to follow the e-Safety rules and to support the safe use of ICT at **Brunswick** School.

Parent/Carers Name		**Pupil Class**	
Signed *(Parent/Carer)*		**Date**	

APPENDIX C

Think then Click

We only go on the internet when we have permission from our teacher or adult helpers.

We only do what we have been asked to do.

If something happens when we are searching for information that is rude, silly or scary we must click on the Big Red Button and report it to our teacher.

If we get stuck or things go wrong we ask for help.
We ask permission to print off information.

We do not put any of our own details onto the computer without permission.

Permission means the teacher says it is ok to do it.

STAFF / GOVERNOR/ STUDENTS (trainee) **APPENDIX D**

ACCEPTABLE USE POLICY AGREEMENT
Brunswick Infant School

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. This applies to ICT used in school and also applies to use of school ICT systems and equipment out of school and use of personal equipment in school or in situations related to their employment by the school. All staff/Governors/visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with **Pierre Crubilier** (e-Safety coordinator) or **Sam Waugh** (Head teacher).

- I will only use the school's email/Internet/Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head teacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address to parents or pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of **Pierre Crubilier.**
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes using school equipment in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head teacher. Images and information on past pupils will be deleted.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Head teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety, Data Protection and Behaviour policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

Staff / Governor / Student - Acceptable Use Agreement

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines. I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Name			
Job Title			
Signed		**Date:**	

APPENDIX E

SOCIAL NETWORKING SITES – FACEBOOK etc
GUIDANCE FOR PARENTS/CARERS

There are many children of Primary School age who have Facebook Profiles despite the permitted minimum age to use the site being 13, according to the site terms and conditions.

Our school is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this particular issue as a concern. Whilst children cannot access Facebook or other social networking sites at school, they could have access to it on any other computer or mobile technology. Websites such as Facebook offer amazing communication and social connections, however they are created with their audience in mind and this is specifically 13 years old. Possible risks for children under 13 using the site may include:

- Facebook use 'age targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered;
- Children may accept 'friend requests' from people they don't know in real life which could increase the risk of inappropriate contact or behaviour;
- Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children;
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own;
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and other options;
- Facebook could be exploited by bullies and for other inappropriate contact;
- Facebook cannot and does not verify its members therefore it important to remember that if your child can lie about who they are online, so can anyone else!
- Some networking sites such as Snapchat can even give precise information about a person's location to other users.

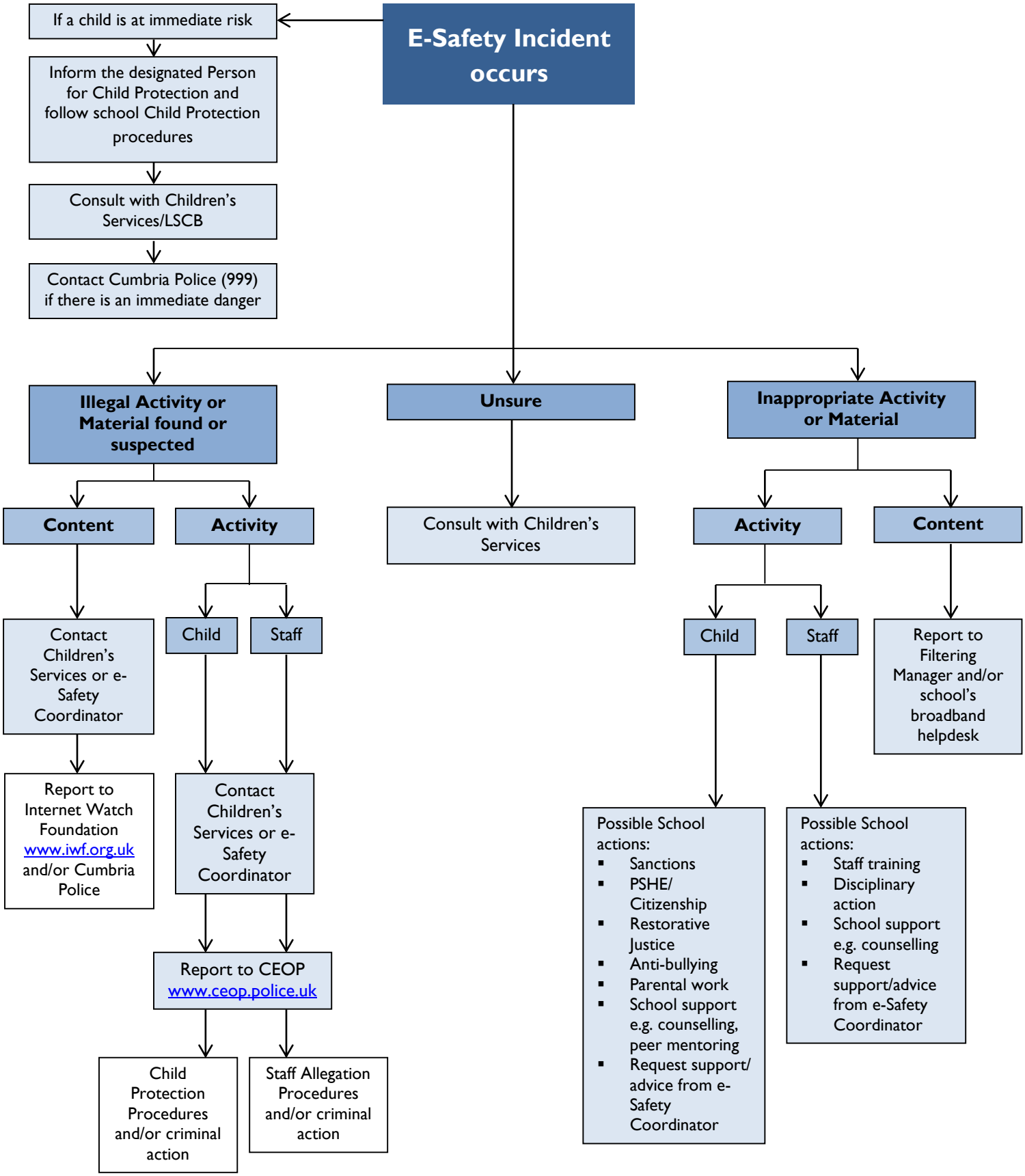
We feel that it is important to point out to parents/carers the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from school and sometimes by a child, their friends, siblings or even parents. We will take action (such as reporting aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children.

Should you decide to allow your children to have a Facebook profile we strongly advise you to:

- Help your child to make their profile safer by having appropriate privacy settings in place. Details of how to do this can be found at http://www.connectsafely.org/pdfs/fbparents.pdf
- Talk to your child about safe and appropriate online behaviour such as sharing personal information or posting offensive messages or photos
- Think about installing the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a CEOP "Report Abuse" button on their Facebook page and has been known to deter potential offenders .
- Get yourself up to speed with the latest guidance and advice. Try www.facebook.com/help/?safety=parents or Connect Safely/iKeepsafe "Facebook Guide for Parents" http://www.connectsafely.org/pdfs/fbparents.pdf
- If you need to play a more active role in your child's online life, you may want to set up your own profile to understand how Facebook works. You may even want to agree with your child to be "friends".
- Make sure your child understands the following guidance:
  - Keep your personal information under control; think, "Would I tell this to a stranger?"
  - Be careful what you share with online "friends" as you may not know all of them well
  - Use "friends lists" to help manage what information you share with whom
  - Be careful what you post; it says a lot about you.
  - Never agree to meet somebody you only know online without telling a trusted adult
  - Always tell someone if you feel threatened or someone upsets you
  - Never write anything you wouldn't be happy for others to see.

We recommend that all parents/carers visit the CEOP ThinkUKnow website for more information on keeping your child safe online Click here to access.

APPENDIX F
RESPONSE TO AN INCIDENT OF CONCERN



Review school e-Safety Policies and procedures; record actions in e-Safety incident log and implement any changes in the future.

X:\policies\health&safety safeguarding\e safety

APPENDIX G

BRUNSWICK INFANT SCHOOL - E-SAFETY INCIDENT LOG

Details of e-Safety incidents to be recorded by the e-Safety Coordinator. This incident log will be monitored termly by the Head teacher, member of SLT or Chair of Governors.

Date	Time	Name of Pupil, Parent or Staff Member	Details of Incident (including Evidence)	Actions and Reasons

E-SAFETY LINKS APPENDIX H

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

- **CEOP (Child Exploitation and Online Protection Centre)**: Click here to access
- **Childline**: Click here to access
- **Childnet**: Click here to access
- **Digizen**: Click here to access
- **Internet Watch Foundation (IWF)**: Click here to access
- **Cumbria Local Safeguarding Children Board (Cumbria LSCB)**: Click here to access
- **Think U Know website**: Click here to access
- **Virtual Global Taskforce — Report Abuse**: Click here to access
- **Information Commissioner's Office (ICO)** Click here to access
- **National Education Network (NEN)** E-Safety Audit Tool: Click here to access
- **Anti-Bullying Network** - Click here to access
- **Cyberbullying.org** - Click here to access
- **Ofcom Report:** Click here to access
- **Learning Curve Education:** Click here to access
- **UK Safer Internet Centre:** Click here to access
- **UK Council for Child Internet Safety (UKCCIS):** Click here to access
- **Wise Kids:** Click here to access
- **Teacher Tube:** Click here to access
- **BBC Teachers:** Click here to access
- **Grid Club**: Click here to access
- **Teem:** Click here to access
- **Sites for Teachers:** Click here to access
- **DfE:** Click here to access
- **Know the Net:** Click here to access
- **Family Online Safety Institute:** Click here to access
- **Facebook Advice to Parents:** Click here to access
- **Test your online safety skills:** Click here to access

BECTA publications *(saved from the National Archives since BECTA's closure in 2011)*

Some of BECTA's guidance documents include:

- E-Safety - Click here to access
- Safeguarding Children Guide - - Click here to access
- Safeguarding Children Checklist - Click here to access
- LSCB Strategy - Click here to access
- Online Behaviours - Click here to access
- Safeguarding Learners - Click here to access

APPENDIX I

LEGAL FRAMEWORK

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 a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Racial and Religious Hatred Act 2006
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.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
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. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming 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 etc. fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should have a copy of The Home Office "Children & Families: Safer from Sexual Crime" document as part of their child protection packs. Click here to access.

Communications Act 2003 (section 127)
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.

Data Protection Act 2018

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). ... They must make sure the information is: used fairly, lawfully and transparently.

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security)
- Accountability.

The Computer Misuse Act 1990 (sections 1 - 3)
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.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

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.

Public Order Act 1986 (sections 17 — 29)
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.

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.

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.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. 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.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"
63 (6) must be "grossly offensive, disgusting or otherwise obscene"
63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/ Bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/antibullying policy.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

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.

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.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

APPENDIX J

GLOSSARY OF TERMS

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology) – *NOTE: Becta Closed in 2011*
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
DfE	Department for Education
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by Naace Click here to access
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network.
KS1	Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups e.g. KS3 = years 7 to 9 (age 11 to 14)
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System

MLE Managed Learning Environment

NEN National Education Network – works with the Regional Broadband Consortia to provide the safe broadband provision to schools across Britain.

Ofcom Office of Communications (Independent communications sector regulator)

Ofsted Office for Standards in Education, Children's Services and Skills

PDA Personal Digital Assistant (handheld device)

PHSE Personal, Health and Social Education

RBC Regional Broadband Consortia have been established to procure broadband connectivity for schools in England. There are 13 RBCs covering most local authorities in England, Wales and Northern Ireland.

SEF Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection

SRF Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark

TUK Think U Know – educational e-Safety programmes for schools, young people and parents.

URL Uniform Resource Locator (URL) it is the global address of documents and other resources on the World Wide Web.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

Appendix K

Prevent Duty Risk Assessment Last reviewed April 2019

No.	Prevent Vulnerability/Risk Area	Risk Addressed Y/N	Action taken to address risk	Any future action required
1	**LEADERSHIP** Do the following people have a good understanding of their own and institutional responsibilities in relation to the "Prevent Duty"? ☐ Governors ☐ Head teacher ☐ Staff	Y	Head teacher and a member of representatives governing body have attended awareness training from the Police, 5th February 2019 All staff have completed the Channel online general awareness training and printed out a certificate to evidence this.	Annual check to ensure any new staff are provided with relevant awareness training Staff training with North Lakes school twilight 9th June 2019

2	**Partnership** • Does the school have a designated member of staff responsible for overseeing the school's response to the Prevent Duty. • Does the designated member of staff know which professionals to liaise with and make referrals to?		Y	School safeguarding procedures cover the school duty and any concern will reported directly to: Prevent@cumbria.police.uk Email. In emergency situations 999 should be called	Check for changes to contact information annually
3	**Staff Training** Do all staff have sufficient knowledge and confidence to: 1) exemplify British Values in their management, teaching and through their general behaviours in the school 2) understand the factors that make people vulnerable to being drawn into terrorism and extremist ideas. 3) have sufficient training to be able to recognise this vulnerability and be aware of what action to take to safeguard children		Y	Much of this is embedded in school practices such as the promise, resilience rucksack, persona dolls, Curriculum Plans and Policies. Any concerns relating to any aspect of safeguarding including exposure to extremist views of any kind should be reported to the head teacher who is the designated safeguarding lead. Whole staff training 5th February 2019 with North Lakes school	Any new permanent staff to undergo Channel General Awareness online training. Temporary Staff and Volunteers will be given information on prevent during induction.
4	**Children's Education linked to British Values** 1) Resilience Rucksack				

	2) Kidsafe Programme 3) Religious Education 4) Social, Moral, Spiritual and Cultural Education 5) SEALS – PSHE + C 6) Persona Dolls 7) School Council 8) National Curriculum (KS1) and EYFS Foundation Stage	Y	British Values are promoted through the school's broad and balanced curriculum, ethos and approach.	
5	**IT (E Safety)** 1) Does the school have a policy relating to the safe use of IT and does it contain a specific reference and inclusion of the Prevent Duty? 2) Does the school employ filtering/firewall systems to prevent staff/students/visitors from accessing extremist websites and material? 3) Is there a procedure to address any breaches of the safety policy? 1. 4) Is e-safety taught in an age appropriate way to pupils.	Y	The school has an e- safety policy and this is reviewed by Mr Crubilier and updates shared with staff annually. Staff, volunteers and parents sign an e-safety form agreeing to comply with the policy. Safety firewalls are in place.	Monitoring of e-safety will be undertaken by the governors, using pupil voice as evidence.
6	**Safeguarding** 1) Is protection against the risk of radicalisation and extremism included within Safeguarding, e safety and the staff code of conduct? 2) Do Safeguarding and welfare staff receive additional and ongoing training to enable the effective understanding and handling of referrals relating to radicalisation and extremism?	Y	See Safeguarding Policy. Shared with Staff re: updates / changes.	Governors to Monitor this.

	3) Does the school utilise Channel as a support mechanism in cases of radicalisation and extremism?		Certificates as evidence of staff completion of Channel General Awareness Training.	
7	**Communications** 1) Is the School's Prevent Lead and their role widely known across the school? 2) Are staff and volunteers made aware of the Prevent Duty, current risks and appropriate activities in this area? **3)** Are there information sharing protocols in place to facilitate information sharing with Prevent partners?	Y	Mrs Sam Waugh – Acting Head teacher and Designated Child Protection Lead is known to be the Prevent Lead. She is responsible for training other staff and volunteers. To share concern with police contact: Prevent@cumbria.police.uk	
8	**Incident Management** 1) Does the school have a crisis management plan which is capable of dealing terrorist related issues? 2) Does the school have effective arrangements in place to identify and respond to tensions in or out of school which might impact upon staff, student and/or public safety?	Y	Crisis Management in place – Mrs Sam Waugh is the Crisis Management Lead.	Crisis Management plan to be reviewed and checked to ensure prevent duty link to dealing with terrorist incidents.
9	**Staff and Volunteers**			

	1) Does awareness training extend to sub-contracted staff and volunteers?	Y	Part of induction process for all staff or volunteers involved in regulated activities.	
10	**Monitoring** 2) Is appropriate monitoring in place to ensure this risk assessment is implemented?	Y	Annual Monitoring – Safeguarding Governors.	