Challenge, Equality & Opportunity

Broadway East First School
Information Security and Acceptable Use of IT Policy 20-21

This policy fully incorporates the 'e-safety Support for Newcastle Schools' developed by the Newcastle Schools' e-Safety group. It has been adapted to include specific measures in place at Broadway East First School in order to ensure all staff, children, governors, parents and visitors are fully informed of their responsibilities relating to these issues. Some technologies referred to in the policy may not be in place at present but their use is included in order to 'future proof' the policy.

1. Scope

This policy applies to:

- All staff users of the school network including all information systems accessed through it; this includes but is not limited to employees, contractors, consultants, external auditors, trainee teachers and temporary/casual staff, including those from private Supply Agencies.
- All children who use the school network, including access to the internet and online resources.
- All other users of the school network, for example visitors who are granted access.
- All the school's information whether held on paper, film, fiche or electronically, and computing equipment, including (but not limited to) computers, servers, iPads, printers, telephones, cameras and hand-held devices such as tablets and 'smart phones'.
- All school owned computing assets including but not limited to laptops, desk tops, iPads and mobile devices.
- All the school's data and all reports derived from such data.
- All programs developed by school employees or on behalf of the school, using school equipment or personal computers used for home working by school employees.
- All communication lines, and all associated equipment or devices used on school premises or connected to school resources that are capable of processing or storing the school's information; this includes all electronic devices used in school whether belonging to the school or personal devices owned by individuals

2. Purpose

This document provides guidance for school staff primarily in the areas of information security and acceptable use. This document complies with recommendations from the Local Authority, ISO 27001:2005 and industry best practice including the Information Commissioner's Office and DFE advice.

Broadway East First School can receive support in implementing this policy from IT Services, IT Assist NE, GEM Education and HR Services at the Local Authority; these services are committed to supporting the protection of the security of the school through the preservation of:

Confidentiality – protecting information from unauthorised access and disclosure.
Integrity – safeguarding the accuracy and completeness of information and processing methods.
Availability – ensuring that information and associated services are only available to authorised users when required.

3. Roles and Responsibilities

The Governing Body has overall responsibility to ensure that the procedure is properly and fairly applied.
The Headteacher is responsible for the ensuring that all staff are aware of this policy and comply with the guidance.
Working under the direction of the Headteacher, the ***Computing Subject Leader*** will be involved in making staff aware of this policy and supporting them in complying with the guidance.
The E-safety Committee, comprising a member of the Governing Body, the Curriculum Leader and the Headteacher, will monitor the implementation of this policy and review its effectiveness annually.

4. Policy Aims

The aims of this Information Security policy are:

- To ensure that all information and information systems on which the school depends are adequately protected to the appropriate level. This includes the IT infrastructure for the retrieval, sharing and dissemination of business critical data and conducting daily transactions.
- To ensure that all staff, children and other users are aware of their responsibility for the security of school information.
- To help staff use information more securely.
- To ensure that all staff and other users are aware of their responsibilities for processing personal information under the Data Protection Act 1998.
- To ensure that all staff users are aware of their accountability and that they are aware that failure to comply with the Information Security Policy is a disciplinary and possibly civil or criminal offence. Any action taken will be in accordance with the relevant school or council disciplinary procedures.
- To ensure that all adult users are aware of their accountability and that they are aware the failure to comply with the Information Security Policy is possibly a civil or criminal offence.
- To make all users aware that the school is legally obliged to inform the police of any illegal activity that takes places on the school premises or using the school equipment.
- To ensure that information assets, computers and communication systems that are owned by the school and supported by IT Assist NE are protected against external and internal threats.

5. Relationship with other policies and procedures

Please also refer to:

- Code of conduct: this sets out the standards expected of staff
- Disciplinary procedure: schools must follow their disciplinary procedure where it is appropriate to take such action against an employee.
- Whistle-blowing policy
- Behaviour Policy (for children in school)
- Safeguarding policy
- Data Protection Act policy/Fair processing notice
- Teacher iPad policy

The experiences and requirements of the various user groups are different, so this policy is divided into three sections. Part A refers to staff users, Part B refers to children at the school, and Part C refers to governors, parents and other visitors.

Part A – Staff Users of the School Network and IT Equipment

A1 Guidance

Staff members represent a key component in the delivery of information security and a secure environment. Investment in secure technology and secure processes is meaningless unless all staff are aware of the role they need to play in security and what is acceptable. The following section outlines areas of personal responsibility for staff members and is intended to provide clear guidance as to the expected role of school staff in providing and maintaining a secure IT/Computing environment in the school. IT Assist NE, GEM Education and IT Services are available to work with the school and individual staff members to provide any clarification, training or support required to ensure that everyone understands their roles and responsibilities.

A1.1 E-safety Awareness and Training

In order to ensure that staff members fulfil their responsibility for IT and Information Security it is essential that appropriate training is provided to ensure an awareness of the legal and procedural expectations placed upon them. To this end, the school and/or IT Assist NE will provide training to all existing staff and to all new members of staff in the form of induction training. A 'refresher' session will be held annually, usually led by Computing Subject Leader, with the support of the Headteacher.

This training will cover the following key areas:

- Known threats, risks and implications
- Acceptable Use
- Password Guidance
- All staff members will be trained and made aware of their personal responsibility for maintaining information security and their roles in the classification process.
- Awareness of this document and any other relevant school policy documents.

A1.2 Acceptable Use

This section is intended to provide staff members with guidance on acceptable and unacceptable use when using information and the computing facilities provided by school and supported by IT Assist NE. If there are any questions or concerns, advice can be sought from the Local Authority and other school advisors. The school's Senior Management Team may be contacted in the first instance if appropriate. Further practical advice on acceptable use can be found in the document 'Becta Dos and Don'ts', a copy of which is saved on the school network (T:/Computing/Policies) and is also available on request from the Headteacher or Computing Subject Leader.

A1.3 Investigations

If there are any concerns that the policies or guidance within this document have been breached, or there is a suspicion of criminal activity then this must be reported directly to a member of the school's Senior Management Team. They will then communicate directly with the Senior Management of IT Assist NE, IT Service and Human Resources to discuss any investigation that may be required. Further specialist advice may be sought from other relevant services within the Local Authority. Breaches of this policy may also result in disciplinary, civil or criminal action. Staff should be aware that school is legally obliged to report any illegal activity which takes place on the school premises or using school equipment to the Police.

A1.4 Using computer equipment

Each user is responsible for the equipment that they use, the data it holds and the output produced. This also applies to portable equipment, media or data that is used away from the normal place of work.

You MUST
▪ Keep any portable equipment securely, and carry it safely.
▪ Keep log on details for resources such as Office 365 and RDS safe at all times and report their loss immediately.
▪ Unless instructed otherwise, log off from the network every night and fully shut down the PC.
▪ Connect laptops to the network at least once a month (and preferably more often) to keep the anti-virus and patching protection up to date.
▪ Report any problems as soon as possible to IT Assist NE (via the reporting form saved on the school network, the Computing Subject Leader or a member of office staff) including the loss of, or damage to, any computing equipment.
▪ Ensure that any redundant computing equipment is disposed of in a secure and legal manner; the Computing Subject Leader, working with office staff, will organise this process as the equipment needs to be disposed of appropriately and removed from the school's equipment list. IT Assist NE can provide support in this process.
▪ Ensure that all software used is correctly licensed and covered by a school or Local Authority license (i.e. not home or personal user). The licence terms for free software must be carefully examined to ensure it meets these requirements.
▪ Ensure all software is installed by IT Assist NE.

You MUST NOT
▪ Connect any non-school mobile devices to the network without the permission of the Senior Management. This includes equipment brought in by visitors, including trainee teachers, other students, presenters, trainers and consultants.
▪ Allow students to use a machine logged on using your or another person's username and password, except when closely supervised e.g. children using the Smartboard with a teacher's laptop attached in a lesson.
▪ Save any information on to any computer or device which is not registered as school equipment.
▪ Change any folder or file's permissions in a way that prevents people from accessing information that they are entitled to see.

You SHOULD
▪ Lock your PC screen (using Ctrl/Alt/Del then 'Lock Computer') whenever you are away from your desk, to prevent someone accidentally or deliberately looking at information, making unauthorised changes, or sending email in your name.
▪ Shut down or logout if you are going to be away from your machine for any length of time.
▪ Report any instances of possible security breaches, including near misses. For example, if: o A colleague is using someone else's log-in name and password. o You can see personal information on a computer screen in an unattended area.

You MUST
▪ only take photographs that are for school purposes using school equipment.
▪ only save photographs of children on the school network and NEVER on any portable device, including USB memory sticks and laptops; photos taken on the iPads should be transferred to the school network as soon as feasible and deleted from the iPad.
▪ Ensure there are no photos on iPads or any other portable device before removing it from the school building (e.g. for teachers to work off site or for use on a school visit).

- ensure permission has been given by parents before using photographs of children on the school website.

You MUST NOT
▪ use personal cameras including mobile phones to take photographs of children from school other than in exceptional circumstances and with prior consent from the Headteacher.
▪ take photographs of children from school out of school, except with prior permission from the Headteacher.

A1.5 Passwords

Effective username and password combinations are a basic security requirement for any information system. But they are only effective if used properly.

You MUST
Choose a password that: ▪ Is at least 8 characters long ▪ Contains at least one letter and at least one numeric character ▪ Contains both uppercase and lowercase letters and at least one punctuation mark or other 'special character' ▪ Where the system cannot meet these requirements you will use the maximum complexity that the system allows ▪ Change your password at least every 90 days (PCs will prompt this). ▪ Change your password as soon as possible, if anyone else gets it know it. Help and support is available through IT Assist NE to support this process.

You MUST NOT
▪ Disclose your password to anyone else. ▪ Use another person's logon name or password or allow someone to use another person's logon name and password. ▪ Use another person's machine whilst they are not there if they have not locked it (log the machine off or lock it for them). ▪ Not use the same password twice. ▪ Write your password down and keep it where anyone else may be able to read or use it. ▪ Reply to any email asking for your username, log in details or password (even with a refusal since this lets the sender know that they have located a valid email address).

You SHOULD
▪ Follow the guidance on permissions. If another member of staff has a **legitimate business** need to view your email account while you are away from school, you should, unless there are unforeseen circumstances, set this up before access is required. Please contact the IT Assist NE for advice and support to help you through this process.

A1.6 Saving files

In order to keep the School's information secure, you should not use the c: drive to save any work related files.

You MUST
▪ Save files on the server rather than on to your PC (including laptops). ▪ Save files to appropriate locations on the network, taking into consideration the access provided to each drive e.g. the Common drive can be accessed by all users. ▪ Use Office 365 to access files from the school network at home or elsewhere. ▪ Restrict access to strictly confidential information on a need to know basis. Help and support is available through the Managed Service to support this process.

You SHOULD
▪ Save your file every few minutes as you work on it.

You MUST NOT
▪ Keep any information on a device in an area where it is particularly vulnerable to theft.

A1.7 Using the internet and email facilities

All network users have access to the Internet and e-mail. By accepting your network account password and related information, and accessing the network, you agree to keep this policy. You also agree to report any network misuse to the IT Assist NE and the School's Senior Management Team. Misuse includes policy violations that harm another person or an individual's property.

The Internet and e-mail systems are provided for business and curriculum purposes. If you are unsure whether an activity constitutes suitable use, you should consult your line manager. To clarify, the email account provided by school should ONLY be used for professional purposes and is NOT for personal use. Any personal email addresses held by members of staff MUST NOT be used for professional purposes.

A1.8 Mobile devices including iPads and laptops

Mobile devices include iPads, laptops and memory sticks and cards, but this list is not exhaustive. Laptops and iPads allocated to teachers are the only type of mobile devices which should be taken off the school premises and only with the permission of the Headteacher. 'One Drive' (part of Office 365) should be used to access files from the school network rather than saving them on mobile devices. In exceptional circumstances, a memory stick may be used with the approval of the Headteacher, but staff members are responsible for ensuring sensitive data, for example personal information, is **NEVER** saved on **ANY** portable device. Sensitive data includes children's names, dates of birth, addresses and IEPs, but there are many other examples of sensitive data in school, if you are unsure you should talk to the Headteacher or the Computing Subject Leader. Specific advice and guidance relating to the use of staff iPads can be found in the Teacher iPad policy.

A1.9 Taking and using photographs and videos of children

At the beginning of each academic year parents/carers will be asked to sign an internet permissions form (See Appendix two). This covers access to the internet, publishing photographs, videos and work. This form covers permission until they leave school at the end of Year 4. Parents/carers sign this form to give permission and are aware that to change permission at any time they must inform the school office. It is the responsibility of all staff to access and check this information whenever they are publishing photographs of children or their work to the internet or to the media/press.

Taking photographs and videos in school is an important source of evidence of achievement and attainment, and also helps share learning and school events with others e.g. by using them on the website and displaying them in school. Guidance on taking photographs and videos is included in this policy for the protection of the children and staff in school. In part this draws on findings from the North Somerset Serious Case Review from April 2012.

- Photos and videos taken in school should be taken with a clear purpose in mind, e.g. recording an activity and achievement, and taken at an appropriate, legitimate time.
- They should show the children in a positive light and be appropriate in terms of children's dress, position and behaviour.
- Photos and videos should be saved onto the school network and deleted from the camera as soon as possible.

- Digital or printed versions of the photos and digital videos should never be taken out of school except in exceptional circumstances and with the approval of the Headteacher.
- Only school devices should be used to take photographs of pupils. There might be exceptions to this such as taking photographs on visits to use on the school's Twitter account, in these cases prior permission must be sought from the Headteacher.

If a member of staff is concerned about the taking and/or use of photographs and videos of children in school MUST report this to a member of the school's Senior Management Team in order to fulfil their professional responsibilities to the children in their care.

Photographs and videos will be used on the school website (www.broadway.newcastle.sch.uk) and school and class Twitter accounts if parental permission has been given. Photographs may also be used in displays around school. Photographs and videos on the website and Twitter will not be labelled with the name of the children, and photographs and videos of the children will not be used if their name is in the accompanying text. The press sometimes publish names with photographs and this is accounted for in the permission form. Photographs and videos will also be uploaded to the seesaw app where they can be added to individual child accounts. These accounts will be archived each year and monitored by the computing lead.

A1.10 Personal responsibility

- Access to the Internet and email during work hours shall be through a school device attached to the network.
- E-mail access is also permitted via the webmail portal or an authorised mobile device.
- Staff should only use approved e-mail systems within school, such as the schools exchange email to send e-mails related to school business.
- Work related information must not be communicated on non-school e-mail systems. The security of data cannot be guaranteed.
- If other staff need to access your email account (for example, during leave or sickness) you should seek help and support on this area is available through IT Assist NE or IT Services.
- No information should be sent via email which is prohibited by the Information Asset Policy of Newcastle City Council. Most school information including children's records fall into the 'Protect' category and if these need to be sent electronically need to be encrypted. Should this be required, advice should be sought from IT Services or IT Assist NE. Information about 'Looked After Children' is 'Restricted' and encrypted email must also be used for this.

A1.11 Personal information

The term 'Personal information' is used frequently in e-safety training and throughout this policy. The term refers to any information that in combination identifies one person to another. This could be a name, address, National Insurance or telephone number. It could also be the type of job they do or the name and location of the school they attend.

- You should take care when sending personal information electronically, this includes uploading or sending information to an Internet site.

A1.12 The security of external communications cannot be guaranteed

Where you have an authorised business need to electronically send sensitive or confidential personal information, which relates to pupils, clients or staff, you must refer to the Information Asset Classification Policy from Newcastle LA. If in doubt, please consult the Headteacher or IT Assist NE.

A1.13 Use of Office 365 (including One Drive) by teaching staff

Access to files from the school network from locations outside school is granted to teaching staff through use of One Drive, part of the Microsoft Office 365 suite. By uploading files prior to leaving the

building, staff are able to access the files when away from school. This is a secure means by which this can occur, significantly more secure than using a laptop's hard drive, a memory stick or an external hard drive which are vulnerable to loss and theft. It also allows access to e-mail away from school.

- Staff members who make use of Office 365 from school should operate to the same acceptable use standards as if they were in school. This includes NOT having personal information including photographs of children stored in this environment. Newcastle LA have assured the school of the high level of security associated with Office 365 (see Subject Leader for further details if required) but files can be downloaded onto other devices and therefore school requires staff not to use Office 365 in this manner.
- You are personally responsible for keeping any work related data stored on any mobile equipment or on Office 365 safe and secure in accordance with the Information Asset Classification Policy from Newcastle LA.

Third party remote access

- Third party suppliers and vendors that require access for support reasons must also utilise the corporate remote access solution. This access also requires that they agree to the corporate Trusted Third Party (TTP) and Non-Disclosure Agreements (NDA).

A1.14 Unacceptable Use

Any use of the internet or IT facilities which is against any relevant legislation or any internal school policies is unacceptable and could lead to disciplinary action. If you are in any doubt about any use, you should contact the school's Senior Management or IT Assist NE.

Examples of unacceptable use include:

- Using 'chat rooms' and 'discussion forums' of a personal, malicious or illegal nature
- Circulating jokes, personal photographs or making malicious comments about other people on 'social networking sites'.
- Deliberate access to or sending any material that is against any of our policies.
- Illegal or malicious use, including downloading or sending copyright material.
- Any form of online harassment (or cyberbullying), including harassment by volume of communications on 'chat rooms', 'discussion forums' or 'social networking sites', or sending 'spam'.
- Creating material containing false claims of a deceptive nature.
- Use for private business purposes.
- Any form of gambling.
- Downloading or distributing pirated software or data.
- Revealing yours or someone else's personal information, such as, home address, telephone number, or financial data.

(This list is not exhaustive.)

Deliberate unlawful or inappropriate material must not be viewed, stored or distributed using the school's IT system or personal devices in school. This can include any material which is in violation of any law or regulation which can be considered by any reasonable person in its context to:

- Be defamatory
- Be violent
- Be offensive
- Be abusive
- Be indecent or obscene
- Incite hatred
- Constitute bullying or harassment

- Breach anyone's confidence, privacy, trade secrets or copyright.

If someone has stated that they do not wish to receive emails from you then you must refrain from sending further emails to them. You must not use the school's email systems for 'spamming' purposes (the use of email to send unwanted/junk/advertising contents to multiple recipients).

- Where possible, IT Services/IT Assist NE will prevent access to material known to be of an offensive or undesirable nature using security tools and filtering software.
- If you receive an email or access a website which you consider to be offensive or potentially illegal, you must report the matter to the Headteacher, Computing Subject Leader or IT Assist NE.
- If you receive an email that you consider to be spam, you should forward it to education.it@newcastle.gov.uk and then future incoming e-mails from that address can be blocked.

A1.15 Personal Use

- Personal use of any computing resource must not involve any unacceptable use.
- Personal e-mail conversations in work time must be as short as possible and kept to a minimum.

Personal use of the internet is allowed outside of working time, for limited periods, or at other times with the Headteacher's approval.

- You should ask the Headteacher if you are in doubt about the acceptability of any personal use.

Access to any IT facilities may be removed or disciplinary action conducted by your employer if you are found to be misusing resources.

A1.16 Personal devices, including mobile phones

Staff members may use personal devices e.g. Smartphones on school premises, provided they are used outside of working time, not in the sight or presence of children, and not used with children from the school. Personal devices must not be connected to the school network and must not be used for professional purposes. To summarise, personal devices are for personal use only and all use of personal devices must comply to this policy when used in school. **When on the school site and using your own mobile phone you must comply to all aspects of Acceptable Use as stated in this policy.**

Mobile phones should not be used as part of classroom practice. They should be stored out of sight of children, e.g. in a bag or drawer; they SHOULD NOT be kept on a teacher's desk. Staff are not allowed to use their mobile phone to take photographs or videos of children in school for any purpose, other than in exceptional circumstances and with prior permission from the Headteacher.

A1.17 Social Networking

Staff members may use Social Networking sites such as Facebook and Twitter for either personal or professional reasons. Forming a Personal Learning Network via social networking sites can lead to significant benefits for their Continuing Professional Development. However, when using sites such as Twitter and Facebook, staff members MUST be aware of the language they use and the comments they make. Privacy settings are not infallible and care should be taken by members of staff to protect their professionalism. The potential audience (e.g. children at the school and their parents, employers etc.) must be considered. It is recommended that comments are not made that would not normally be shared publicly with these groups.

Staff members should not allow access to their own personal areas or open lines of communication with students via social networking sites. It is very important that staff members maintain professional relationships with students at any time and this would be compromised by allowing students access to personal information or photographs. If you do have any current or former pupils including those who may be post-16 students now, as contacts, please remove them to protect yourself as a professional.

Use of Social Networking sites for school business (e.g. sharing information with parents, promoting the school etc.) must be through use of a school account e.g. a class account on Twitter or a class or school blog.

A2 Monitoring

IT Services or IT Assist NE will, if requested, facilitate the monitoring of Internet and E-mail facilities and their usage, on behalf of the school to highlight non-compliance. This monitoring will include, but will not be limited to:

- All internet sites staff browse
- All transactions staff make via the internet
- All files downloaded or uploaded to or from the internet
- All e-mails sent and received
- All attachments sent and received

Therefore staff should not expect privacy on any e-mails that are sent or received, or websites visited.

Logs are retained on all emails that are sent and received as well as all websites that have been browsed by any user. IT Assist NE or IT Services may be required to disclose any information kept on computer systems to outside parties or law enforcement authorities. This would always happen in consultation with the school's Senior Management.

A3 Sanctions

Failure to comply with any of the requirements of this policy may result in further action being taken by the school/local authority in line with the appropriate disciplinary policy. Instances of non-compliance with this policy shall be identified, documented and escalated. Remedial measures shall be implemented by IT Assist NE and school's Senior Management Team as quickly as possible. Deliberate non-compliance by individuals, whether they are system administrators or other users, shall be treated as a disciplinary offence, and may also result in civil or criminal action being taken.

Violations of established security procedures and inadvertent and deliberate compromise of School proprietary and personal information are actions that are adverse to the security of a school and as such may warrant disciplinary, civil or criminal action, based on the severity of the incident.

Some breaches of this policy may result in loss of data such as personal information, and this must be reported to the Information Commissioner's Office. The loss is publicly declared and the loss of equipment and/or data must be explained, with the school being held responsible.

Part B – Children using the School Network and IT Equipment

B1 Guidance

This part of the policy outlines the school's purpose in providing an IT network (including internet access and email facilities) for children at Broadway East First School. It also explains how the school seeks to avoid the potential problems that unrestricted Internet access could give rise to. The policy

applies to all children who are pupils at Broadway East, but also applies to members of staff when using the internet with the children.

B2 Internet Access in School

Providing access to the Internet in school raises educational standards and enhances learning opportunities. All PCs, laptops, netbooks and iPads in school have internet access and children will use the internet to complete tasks related to their work in a range of curriculum areas. It is the responsibility of staff to check the internet permissions for their class prior to allowing children to access the internet in school. Children in Key Stage 2 may use e-mail and all classes will also use Twitter to share their learning with others. Access is available to web sites worldwide (including museums and art galleries) offering educational resources, news and current events.

Staff, including supply staff, are not expected to take charge of an internet activity without any necessary training or support. Staff members are given opportunities to discuss issues and develop good teaching strategies. Permanent members of staff will be provided with training and a full copy of this policy. Visitors such as supply teachers, trainee/student teachers and guest speakers who require access to the school network will be required to read an abbreviated version before working with children to ensure they are fully protected. A full version of this policy is available for parents and others to read on demand from the school office or on the school website.

B3 Ensuring internet access is appropriate and safe – 'e-safety'

The internet, as a communications medium, is available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher, and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- our internet access provides a service designed for children including a "firewall" filtering system intended to prevent access to material inappropriate for them;
- children using the internet will be working in the classroom or other learning environment, during lesson time and will be supervised by an adult (usually the class teacher) at all times;
- staff will check that the sites pre-selected for use by the children are appropriate to the age and maturity of pupils;
- staff will be particularly vigilant when children are undertaking their own search and will check that the they are following the agreed search plan;
- children will be taught to use 'the internet' in all its forms responsibly in order to reduce the risk to themselves and others;
- our the rules for 'Responsible Use of the laptops and iPads' will be posted in every classroom, taught to children at the beginning of the school year, and then revisited at appropriate points throughout the year;
- the Computing Subject Leader will monitor the effectiveness of internet access strategies;
- the Computing Subject Leader will ensure that occasional checks are made on files to monitor compliance with the school's Internet Use Policy;
- the Headteacher will ensure that this aspect of the policy is implemented effectively;
- methods to quantify and minimise the risk of children being exposed to inappropriate material will be reviewed when developments occur and advice from the Local Authority, our Internet Service Provider and the DFE will be sought.

It is the experience here and in other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. ***Neither the school nor Newcastle LA can accept liability for the material accessed, or any consequences thereof.***

A most important element of the rules for 'Responsible Use of the School Computers' is that pupils will be taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable, or receive an inappropriate email.

In the unlikely event that an incident in which a child is exposed to offensive or upsetting material occurs, the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children will be taken by the Computing Subject Leader and the Child Protection Officer in consultation with the Head Teacher and the child's class teacher. All teaching staff and the E-safety Committee will be made aware of the incident if appropriate.

In the unlikely event that one or more pupils discover (view) inappropriate material, the first priority will be to give them appropriate support. The children's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and children to resolve any issue. If staff or children discover unsuitable sites the Computing Subject Leader will be informed and the incident will be logged. The Computing Subject Leader will report the URL (address) and content to IT Services and seek advice from them; if it is thought that the material is illegal, after consultation with IT Services, the site will be referred to the Police.

The children are expected to play their part in reducing the risk of viewing inappropriate material by obeying the rules for 'Responsible Use of the laptops and iPads', which have been designed to help protect them from exposure to internet sites carrying offensive material.

The following table clarifies the procedure that will be followed should an e-safety incident occur:

Sequence	Events
1	Child(ren) views inappropriate material or receives inappropriate message, and reports it to a member of staff. (This may include use of 'Hector' to shield the screen.)
2	Member of staff investigates the report and if possible views the material or message, without exposing the child(ren) to it any further.
3	The child is supported throughout this process, by another member of staff if necessary.
4	If the report is substantiated, the member of staff will immediately report it to the Computing Subject Leader and/or the Headteacher.
5	The Computing Subject Leader or the Headteacher follows up the initial investigation and views the material, with the aim of identifying the source. (If the Computing Subject Leader has completed this stage of investigation, the Headteacher will always be informed at this stage at the latest.)
6	The Computing Subject Leader or the Headteacher will inform IT Assist NE and IT Services and discuss further action, including possible involvement of the police and other authorities.
7	Parents will be informed about the incident and the response which has taken place. (This may take place earlier in the process, for example if the incident occurred close to the end of the school day.)
8	The incident will be recorded on the E-safety Incident Log, stored electronically on the school network (T:Computing/Esafety)
9	The Computing Subject Leader or the Headteacher will inform members of the E-safety committee, teachers in order to begin the process of improving practice and protective measures.
10	A review of security measures and e-safety practice, including this procedure, will take place, led by the E-safety Committee, who will also inform The Governing Body of the incident and outcome of the review.

B4 Maintaining the security of computers connected to the internet

Connection to the internet significantly increases the risk that a computer may be infected by a virus or accessed by unauthorised persons. IT Assist NE regularly updates virus protection for the network and the Computing Subject Leader will keep up-to-date with new developments and work with IT Assist NE to ensure security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary. Children and staff also play important roles in maintaining the security of the school's network. Passwords and other security information should not be shared, and files and folders belonging to others should not be accessed without permission.

B5 Using the internet to enhance learning

Pupils will learn how to use a web browser and suitable web search engines so they can access the internet to find and evaluate information. Access to the internet should be a planned part of the curriculum that will enrich and extend learning activities and will be integrated into medium-term and short-term planning. As in other areas of their work, we recognise that pupils learn most effectively

when they are given clear objectives for internet use. Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed:

- access to the internet may be by teacher demonstration;
- children may be given a suitable web page or a single web site to access;
- children may be provided with lists of relevant and suitable web sites which they may access;
- more experienced children may be allowed to undertake their own internet search having agreed a search plan with their teacher; pupils will be expected to observe the rules for 'Responsible Use of the laptops and iPads' and will be informed that checks can and will be made on the sites they access.

Children accessing the internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the internet once they have been taught the rules for 'Responsible Use of the laptops and iPads' and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the internet.

In addition, parental permission must be granted before children use the internet to support their learning.

B6 Using information from the internet

We believe that, in order to use information from the internet effectively, it is important for children to develop an understanding of the nature of the internet and the information available on it. These Digital Literacy skills are important for the children now, but are also life skills which are important for the children's future. In particular, they should know that, unlike the school library for example, most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited or edited and most of it is copyright protected.

- Children will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- Whenever it is appropriate, teachers will teach 'Digital Literacy', ensuring that children are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium);
- When copying materials from the Web, children will be taught to observe copyright protections;
- Where appropriate children will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

B7 Using the school's email system

In Key Stage 2, children may use the school's email system, but children do not have individual email accounts, and are not given the log on details for the class account. Typically the class' email account would be used by the teacher working with the class.

It is important that all communications are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

- children will only be allowed to use e-mail once they have been taught the rules of 'Responsible Use of the laptops and iPads', the reasons for these rules and the sanctions available for misuse of email, the internet or the Twitter account;
- teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using email and the internet;
- children may send e-mail as part of planned lessons but will not be given individual e-mail accounts;
- in-coming e-mail to class email addresses will not be regarded as private;

- children will have any email messages they compose checked by a member of staff before sending them;
- the forwarding of chain letters will not be permitted;
- children will not be permitted to use email at school to arrange to meet someone outside school hours.

B8 Twitter accounts

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and some staff are users of networks such as Facebook, Twitter and blogs, using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

Twitter is used by all classes. It is essential that appropriate educational use of Twitter is achieved and that the good name of the school is maintained. Access to Twitter will only be given to children in school using a class username and all 'tweets' must be viewed by the class teacher before they are posted to ensure they are accurate, cannot be misconstrued and maintain the good name of the school.

B9 Broadway East First School Web Site

Our school web site is intended to:

- provide accurate, up-to-date information about our school;
- enable pupils to publish work to a high standard, for a very wide audience including pupils, parents, staff, governors, members of the local community and others;
- celebrate learning and progress;
- promote the school.

All classes contribute to the school web site. Class teachers are responsible for ensuring that the content of the pupils' work is accurate and the quality of presentation is maintained. All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status. All teachers are now involved in adding material to the website, and are therefore responsible for up-loading pages to the school web site and ensuring that any links work and are up-to-date.

The point of contact on the web site will be the school address, telephone number and e-mail address. We do not publish pupils' full names or photographs that identify individuals on our web pages. Home information will not be published. Permission will be sought from individuals from outside the school before they are referred to by name on any pages we publish on our web site.

Parental permission MUST be given before any photographs of a child or their 'work' is published on the school website.

School website address: **www.broadway.newcastle.sch.uk**

B10 iPads and Apps

Children in school will have access to iPads which have a range of appropriate, educational apps on to support learning. Each class in school will have their own seesaw account which will be accessible through staff and children's iPads. Each class will have their own QR code to access their class page however these will not be on display in the classroom and will only be given to children when necessary. Children will only be able to see work in their class which the teacher has accepted. Children will be able to upload photographs from the iPad to seesaw and take photographs/videos on the app. The class teacher will have responsibility for checking work which the children post and giving feedback on this.

Wherever possible, children will be taught how to delete photographs which they have taken off the iPads before the end of the lesson or as soon as possible thereafter.

B11 Sanctions

If the privileges of access to the internet, VLE, blog or use of e-mail facilities are abused by failing to follow the rules that have been taught, then sanctions consistent with our Behaviour Policy (refer to Behaviour policy) will be applied. This may involve informing the parents/carers. Teachers may also consider whether access to IT facilities in school may be denied for a period. The sanctions which are likely to be applied are as follows, however individual circumstances will determine the exact sanction that would be used.

Category	Example of behaviour	Typical sanction
Minor abuse of privileges	Searching for inappropriate content on the internet(off topic research; more silly than offensive)	Verbal warning about future use of the computing facilities
Medium abuse of privileges	Deliberately searching for inappropriate content on the internet Abuse of the email system	Verbal warning, and parents informed
Serious abuse of privileges	Repeat of earlier abuse of privileges	Temporary suspension of use of IT facilities
Persistent abuse of privileges	Repeat of earlier abuse of privileges after already receiving a temporary suspension of use computing facilities.	Permanent suspension of use of IT facilities

Part C – Governors, Parents and Visitors using the School Network and Computing Equipment

C1 Access to the school network for Governors, Parents and Visitors

Governors, parents and other visitors to school may need access to the school network. For example a visiting speaker may need to show a presentation on a Smartboard or use a website, a Governor may use a school PC to complete a task related to their role, or a parent helper may be making resources while helping in school. For this reason, a 'visitor' account has been set up. If use of the school network is needed, the Governor, parent or visitor will be asked to read an abbreviated version of this policy, with a full version being available on request, and if they agree to adhere to it, they will be given a user name and password. The abbreviated version of the policy will refer to the relevant sections of this policy (see below).

C2 Access to the school network for Trainee/Student Teachers

The school often hosts trainee or student teachers on placements which form part of their Initial Teacher Training (ITT). Trainee or student teachers require access to the school network as part of their teaching commitments and to complete their professional studies. Each trainee will be given an individual user name and password to enable them to access the school network and the internet. They will not be given a school email address. The account will also provide access to a network drive where they may save files. As well as subject to the monitoring described in Part A, the network drive provided will also be accessible to the Computing Subject Leader and the Headteacher for monitoring purposes.

C3 Working with children using PCs

If Governors, parents or other visitors are working with children using computers or iPads, particularly if they are using the internet, they should be made aware of the importance of e-safety and the rules children follow. If they become aware of children viewing any inappropriate content, they MUST inform the member of staff they are working with or the Headteacher.

C4 Taking photographs

Visitors to school may not take photographs of the children without first requesting and receiving permission from the Headteacher. Unless the Headteacher decides differently, permission is given for parents to take photographs and record videos of children performing in class assemblies, the Year 4 leavers' assembly, Christmas concerts and any other performances; this is on the understanding that these are for personal use only.

C4 Relevant sections of this policy

The following sections from Part A of this policy are also apply to Governors, parents and other visitors, and as such they should be made aware them: A1.3, A1.4, A1.7, A1.8, A1.9, A1.14. A1.15, A1.16 and A2.

C5 Sanctions

While not subject to disciplinary procedures due to the nature of their role, any visitors who breach this policy may be subject to civil or criminal action, and they should be aware that school is obliged to report illegal activity taking place on school premises or using school equipment to the Police.

6. Monitoring and review

The policy will be reviewed on an annual basis by the E-safety Committee to ensure it is appropriate in light of recommended best practice and complies with statutory regulations. In the event of any conflict with statutory regulations, the legal provisions will have precedence over this procedure in all cases.

The E-safety Committee, reporting to the Governing Body, will monitor the application of this policy and procedure, particularly to ensure that the school's practices comply with it. This will primarily take the form of an e-safety walk around school looking for good practice being observed as well as any breaches of this policy. This will take place annually, prior to refreshing e-safety training to determine where the focus of the training needs to be.

Date reviewed: Autumn term 2019
Review date: Summer term 2020

APPENDIX ONE: rules for Responsible use of our school laptops and iPads for Key Stage 2

Responsible use of our school laptops and iPads

- At all times, I will think before I click (especially when deleting or printing).
- When using the internet, I will think about the websites I am accessing.
- If I find a website or image that is inappropriate, I will inform my teacher straight away.
- When using information or pictures from websites, I will try and say which website it came from.
- When communicating online, I will think about the words that I use and will not use words that may offend other people.
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number.
- I understand that people online might not be who they say they are.
- I will not look at other people's files or documents without their permission.
- I will not log on using another person's account.
- I will think before deleting files.
- I will think before I print.
- I know that the teachers can, and will, check the files and websites I have used.
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers.
- I understand that if I am acting inappropriately then my parents may be informed and I may not be allowed to use the computers at school.

The Golden Rule:

Think before you click

APPENDIX TWO: rules for Responsible Use of the laptops and iPads for Reception and Key Stage 1

Responsible use of our school laptops and iPads

The Golden Rule: Think before you click

☺ I will follow clear instructions from my teacher when using the internet.

☺ I will only use the internet when a teacher is with me.

☺ If I see something that upsets me, I will tell a teacher.

☺ I will think before I print or delete.

☹ I won't look at or delete other people's files.

☹ I won't log on using someone else's username.

☹ I won't complete forms on the internet or share personal information with others on the internet.

I know that if I deliberately break any of these rules, I may not be allowed to use the computers and my parents may be informed.

KS 2 Responsible use of our school laptops and iPads

- At all times, I will think before I click (especially when deleting or printing).
- When using the internet, I will think about the websites I am accessing.
- If I find a website or image that is inappropriate, I will click Hector the dolphin to cover the screen and tell my teacher straight away.
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site.
- When communicating online, I will think about the words that I use and will not use words that may offend other people.
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number.
- I understand that people online might not be who they say they are.
- I will not look at other people's files or documents without their permission.
- I will not log on using another person's account.
- I will think before deleting files.
- I will think before I print.
- I know that the teachers can, and will, check the files and websites I have used.
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers.
- I understand that if I am acting inappropriately then my parents may be informed and I may not be allowed to use the computers at school.

The Golden Rule: **Think before you click**

R and KS1 Responsible use of our school computers

☺ I will be careful when going on the internet.

☺ I will only use the internet when a teacher is with me.

☺ If I see something that upsets me, I will click Hector the dolphin to cover the screen and then tell a teacher

☺ I will think before I print or delete.

☹ I won't look at or delete other people's files.

☹ I won't log on using someone else's username.

☹ I won't complete forms on the internet or share personal information with others on the internet.

I know that if I deliberately break any of these rules, I may not be allowed to use the computers and my parents may be informed.

The Golden Rule: **Think before you click**

APPENDIX TWO: INTERNET PERMISSIONS

September 2020

Dear Parents,

Using the Internet at Broadway East

Welcome to the new school year. We would like to share the following information about internet use at Broadway East with you.

How the internet is used at school

- We provide supervised access to the Internet as part of the school curriculum, including the development of computing skills.
- We believe that the use of the internet is worthwhile and part of the essential skills for children as they grow up in the modern world. Classes will also use Twitter to share their learning with others.
- We have taken positive steps to minimise the risk of access to undesirable materials. This includes a filtering system and firewall provided by the Internet Service Provider. (This may not be the case at home and we can provide references to information on safe Internet access if you wish.) Children are also taught a set of rules for using the computers in school responsibly, a copy of which is attached.
- In accordance with good practice, we need your permission for your child to use the internet in school.

NB Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities. A full copy of our Information Security and Acceptable Use of IT Policy is published on the school website, and a paper copy is available on request from the school office or the Computing Subject Leader.

Our school website, use of photographs and video

- Our school website address is www.broadway.newcastle.sch.uk.
- It is continually developing and is an exciting opportunity to share information about children's learning and our school, and also to promote the school to the wider community.
- We use activities completed by the children, photographs and videos of the school and activities which take place in school on the website, and these may include children. We do not publish pupils' full names or photographs that identify individuals on our web pages. A child in a photograph would never be named, unless it was in exceptional circumstances and only with parental permission. School performances may be filmed, used in school and possibly sold as a fundraising activity.
- We consider ourselves to use images responsibly and appropriately, but we need your permission to use photographs and video of your child on the website and to publish their work.
- If you have any concerns about this, please look at the school website to see how images are used and also discuss your concerns with me or another member of staff before making your final decision. It may reassure you to know that it is usually difficult to identify individuals on the website as the children mostly appear in groups, often facing away from the camera while completing an activity. Around 95% of parents agree to photos of their child being used.

The attached permission form asks for permission for:

- Your child to use the internet
- For their work to be used on the school website and Twitter
- For their photograph/video to be used on the school website and Twitter
- For their photograph to be used in the media, press and publicity materials

This permission is sought for the time your child is at Broadway East First School (usually the end of Year 4). Should your wishes change during this time, please inform school of this as soon as possible.
Please complete the attached form and return it to school. If you decide not to give permission for any of the above, please inform your child's class teacher so we can ensure your wishes are fulfilled. If forms are not returned, school staff will have to contact you and this wastes valuable time. Should you wish to discuss any aspect of Computing or Internet use, please telephone school to arrange an appointment with me or Ms McKenna.

Yours sincerely

Using the internet and use of images at Broadway East

(from September 2020 until my child leaves the school)

Please sign and return this form to school as soon as possible.

NAME OF CHILD _____ CLASS _____

USING THE INTERNET

I have read and understood the school rules for Responsible Use of our School Computers.
I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials, and that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

I give permission for my child to access the Internet.

Signed _____Please print name _____

PUBLISHING WORK ON THE INTERNET

I agree that, if selected, my son/daughter's work may be published on the Internet, including the school website and Twitter.

Signed _____Please print name _____

PUBLISHING IMAGES/VIDEOS ON THE INTERNET

I give permission for photographs/videos including my child to be published on the school website and Twitter and included in recordings of school performances.

Signed _____ Please print name _____

USE OF PHOTOGRAPHS IN MEDIA, PUBLICITY AND PRESS

We sometimes use children's photographs in the local press, training materials for schools and other institutions.

I give permission for photographs including my child to be published in the press and in other printed publications.

Signed _____ Please print name _____

Please note: We never publish photographs with full names but the press often do even when directed otherwise, therefore by giving permission to use your child's photographs in the press you must also be giving permission to use his or her names.