Boundary Primary School

Online Safety and Digital Data Policy

Amalgamating the ICT Acceptable use, Online Safety Charter, Use of Photographic and Video Images Policy.

To be read alongside our Code of Conduct; Policy for all Staff and Volunteers; and Teacher Standards Section B regardless of job role.
This policy is maintained regularly by Boundary Primary School and will be used as evidence in the event of any breach, along with the Code of Conduct.

Review period: Annually
Date policy last reviewed: June 2020
Person Responsible for Policy: Computing Co-ordinator

Contents:

Introduction, Prevent Duty and CSE 3
ICT Security 5
Virus, Managing Passwords 5
Monitoring 6
Security Breaches and Incident reporting 7
Email 8
Sending Emails and Receiving emails 8
Managing Emails and Pupil emails 9
Emailing Personal Information 10
Online Safety 11
Roles and Responsibilities and the Online Safety Curriculum 11
Pupils with Additional Needs, Online Safety for Staff, Managing the message 12
Incident Management, Misuse and Infringement 13
Internet Access 14
Internet Do’s and Don’ts 14
Internet Use 15
Managing other Internet Technologies 16
Parental Involvement 17
Social Media 18
Data Security 19
Security and Protective Marking 19
IRO/IAO 20
Protecting Personal/Confidential Information, Remote Access 21
Images and Film, Publishing 22
Webcams and CCTV and Videoconferencing 23
ICT Equipment and Infrastructure 24
Servers, Portable Equipment, Removable Media 25
Telephone Services, Mobile phones for pupils 26
Mobile Phones for staff, Disposal of redundant equipment 27
Writing and Reviewing this Policy 28
Appendix 1: Acceptable Use Policy for Pupils 29
Appendix 2: Acceptable Use Policy for Staff and Governors 30
Appendix 3: Acceptable Use Policy for Visitors and Volunteers 33
Appendix 4 – Additional measures and guidance for periods of School Closure 34
Online Safety in Brief 35
Boundary Online Safety Charter 36

Introduction

Boundary Primary School (referred to as the School) will try to ensure that its staff and volunteers will have quality access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

This AUP details ways in which ICT facilities can and cannot be used at our School. It should balance the desirability of fully exploiting the potential of digital resources for learning and teaching and communication with safeguards against the risks and unacceptable activity.

Ultimate responsibility lies with Governors who delegate the responsibility to the Headteacher to manage and enforce this policy. The Governing Body takes its responsibilities in providing excellent ICT facilities and its responsibilities for protecting staff and pupils very seriously.

While the Internet and electronic mail are excellent resources for teaching, learning and communication, inappropriate use will be considered a disciplinary matter or even lead to prosecution. In providing a safe, secure and effective learning and teaching environment, the Headteacher, acting on behalf of the Governing Body, may monitor the use of digital systems across the School, including networked and non-networked devices.

The computer network is owned by Boundary Primary School and is available to learners to further their learning and to staff to enhance their professional competence including teaching, research, administration and management. Our Internet Access Policy has been drawn up to protect all learners - Pupils, Staff, Governors and other authorised users.

The Headteacher, acting on behalf of the Governing Body, reserves the right to examine or delete any files that may be held on its digital system or to monitor internet activity.

Staff requesting Internet access will read this policy and sign to say they understand it. Non signing will result in access to computers and other digital media being denied.

There are many occasions on which it is a good thing to make use of photographs and video images that include children. This is perfectly proper and to be encouraged. However, our school will do all it can to ensure that images are used properly, and that, as in all matters, risks are minimised, and our children kept safe and secure, whether at Boundary Primary School or elsewhere. The aim of this policy is to establish the right balance between the proper use of technology and the safety of our children at all times.

Under the terms of the Data Protection Act 1998, all photographs and video images of children and staff alike are classified as personal data. This means that no image can be used for display or for school publicity etc., unless consent is given by or on behalf of the individual concerned.

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 information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

All users should have an entitlement to safe internet access at all times

Aims and Objectives.

Through the implementation of this policy, we aim to:

- ✓ Ensure that the achievements and activities of children in Boundary Primary School can be celebrated through photographs and visual records without in any way compromising their safety;
- ✓ Comply fully with the requirements of the Data Protection Act 1998.
- ✓ Comply fully with KCSIE 2020
- ✓ Staff and volunteers will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- ✓ School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- ✓ Staff are protected from potential risk in their use of ICT in their everyday work.

Prevent Duty and CSE

In line with Boundary Primary School Prevent Risk Assessment, all staff should be aware of children becoming radicalised through the use of the internet.

- Staff are aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people are warned of the risks of becoming involved in such groups.
- Blackpool Council and Boundary Primary School ensure that adequate filtering is in place, with a review of filtering taking place whenever there is any incident of a young person accessing websites advocating violent extremism.
- Teachers monitor and ensure that children are directed to appropriate websites.
- Incidents are reported to the Designated Safeguarding Leader as soon as possible, and record through MyConcern, in line with the Prevent Policy.

Child Sexual Exploitation (CSE) describes situations where a young person takes part in sexual activity either under duress or in return for goods, food or accommodation. A key element of CSE is that there is a power imbalance in the relationship, for example often the perpetrator is much older than the child, who may not aware that they are being abused.

- Staff are aware that children can be sexually exploited on-line, for example posting explicit images of themselves in exchange for money or goods.
- If staff are concerned that a child they work with is being sexually exploited on-line, they report this to the Designated Safeguarding Leader immediately, and record this on MyConcern.

ICT Security

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using pre-installed School provided anti-virus software before being used. All downloads and attachments that staff use on school provided equipment should be appropriate and relevant to the context of the school.

- Never interfere with any anti-virus software installed on Boundary Primary School equipment that you use.

- If your machine is not routinely connected to the School network, you must make provision for regular virus updates through the ICT technician.

- If you suspect there may be a virus on any Boundary School equipment, stop using the equipment and contact ICT support immediately. You will be advised what actions to take and they will be responsible for advising others that need to know.

- Staff are not permitted to bring in their own equipment and use it in class, unless it has been checked and verified by ICT support in school. Staff are aware of this.

Managing Passwords

- **Always use your own** personal passwords. Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.

- Staff should change temporary passwords at first logon.

- Change passwords whenever there is any indication of possible system or password compromise. Staff should ensure that periodically they change their passwords.

- Do not record passwords or encryption keys on paper or in an unprotected file.

- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

- **Never tell a child or colleague your password.**

- **If you aware of a breach of security with your password or account inform a member of the SLT or ICT technician immediately.**

- Personal passwords must contain a minimum of six characters and be difficult to guess.

- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.

- User ID and passwords for staff and pupils who have left the School are removed from the system within 48 hrs.

- **If you think your password may have been compromised or someone else has become aware of your password report this to the ICT technician.**

- **Emailed documents containing data should be password protected.**

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact a member of the senior leadership team (SLT). Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Boundary Primary School business related information; to confirm or investigate compliance with Boundary policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account, where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.
Please note that personal communications using Boundary ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the School’s internet provider and these logs may be monitored by ICT authorised staff.

Security Breaches

A breach or suspected breach of policy by a Boundary School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the Code of Conduct.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's Office (ICO) has powers to issue monetary penalties up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the ICO are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the ICO with specified
- information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act,
- requiring organisations to take (or refrain from taking) specified steps in order to ensure
- they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good
- practice,
- Report to Parliament on data protection issues of concern.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to Boundary Primary School SLT or Computing Co-ordinator. Similarly, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher.

E-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of Boundary Primary School, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette.

Sending emails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, please refer to the Code of Conduct.
- Use your own Council e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily.
- Whenever possible, send the location path to a shared drive rather than sending attachments
- Boundary/Google e-mail is not to be used for personal advertising.
- **When sending an email externally that contains data, ensure that the document is password protected and that the password is sent in a separate email to the recipient.**
- **In line with GDPR guidance, if staff are sending external emails they are now to use BCC to ensure other email address remain anonymous.**

Receiving emails

Check your e-mails regularly.

Never open attachments from an untrusted source; Consult the ICT technician first.

Do not use the e-mail systems to store attachments. Detach and save business related work to an appropriate shared location.

The automatic forwarding of chain e-mails is not allowed.

In line with GDPR guidance, emails should be deleted when they are not needed and any that are required should be saved into a sub file. Emails over 12 months old should be deleted if they are not in a sub file.

There is additional guidance in relation to the sending and receiving of emails in Appendix 4 of this policy for periods of school closure such as the period during the Covid-19 Pandemic in 2020.

Managing email

The School uses Blackpool Google Mail to provide all staff with their own account to use for all Boundary School business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered by Blackpool Borough Council and logged; if necessary, e-mail histories can be traced. The School email account should be the account that is used for all School business, the only exception to this is your teacher*class*@boundary.blackpool.sch.uk email address which can be used with prior permission from SLT.

Under no circumstances should staff contact pupils, parents or conduct any School business using personal e-mail addresses.

All e-mails should be written and checked carefully before sending, in the same way as a letter written on Boundary headed paper.

Staff sending e-mails to external organisations, when not part of their day to day duties should inform their line manage.

Pupils may only use Boundary approved accounts on the School system and only under direct teacher supervision for educational purposes.

E-mails created or received as part of your job role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

- Delete all e-mails of short-term value.
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.
- The forwarding of chain letters is not permitted.

Pupil emails

Pupils will be issued with a pupil email account, based on the Year group curriculum needs. All pupil e-mail users are expected to adhere to the generally accepted rules of ‘netiquette’, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication or arrange to meet anyone without specific permission. Parents will have signed the Digital Permissions Data Sheet to ensure that Pupils are allowed to use the email.

Pupil emails are set up and controlled by Blackpool Borough Council, any issues around logging in to pupils’ email accounts need to be raised through ICT Technician or the Computing Co-ordinator.

- Pupils must immediately tell a teacher / trusted adult if they receive an offensive e-mail.
- Staff must inform the Headteacher and ICT technician if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the ICT/Computing Scheme of Work.
- Pupils are reminded of online safety during sessions involving emails.

□

However and wherever you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all policies apply.

Emailing Personal, Sensitive, Confidential or Classified Information

Where your conclusion is that e-mail must be used to transmit such data:

Obtain express consent from a member of the SLT to provide the information by e-mail.
Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Encrypt and password protect your laptop. If in doubt, discuss with the ICT technician.
- 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 any more recipients than is absolutely necessary.
- Do not send the information to any body/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.
- When sending external emails, use BCC instead of CC.

Online Safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

- **Contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Online Safety Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within Boundary Primary School, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All members of the School community have been made aware of who holds this post. It is the role of the Computing Subject leader to ensure that Curriculum updates are inline with best Online Safety Practice. It is the role of the Headteacher, Computing Lead teacher and Designated Safeguarding Lead to oversee and keep up to date with Online Safety changes.

SLT and governors are updated by the Headteacher and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the School's acceptable use agreements for staff, governors, parents, visitors and pupils, is to protect the interests and safety of the whole School community. It is linked to the following mandatory policies: Code of Conduct, child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

Online Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety.

Boundary Primary School has a Computing curriculum, which embeds the teaching of Online Safety.
Educating pupils about the online risks that they may encounter outside the school is done informally when opportunities arise and as part of the Online Safety curriculum.

Pupils are to learn about the relevant legislation when using the internet, such as data protection and intellectual property, at an age appropriate level, which may limit what they want to do but also serves to protect them.

Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities.

Pupils are taught about of the impact of Cyber bullying and know how to seek help if they are affected by any form of online bullying. Pupils are made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent / carer, teacher / trusted staff member, or organisations such as Cyber mentors, Childline or CEOP report abuse button. The School website offers links to advice and support for children and parents.

Pupils are taught to critically evaluate materials and learn good searching skills through cross -curricular teacher models.

Pupils with Additional Needs - Equal Opportunities

Boundary Primary School endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the School Online Safety Charter. See Appendix 1.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

Online Safety Skills Development for Staff

Staff receive regular information and training on Online Safety and how they can promote the 'Stay Safe' online messages.

New staff receive information on the School's acceptable use policy as part of their induction.

All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community (see flowchart in Appendix 2)

All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

Managing the Online Safety Messages

We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used.

The Online Safety Curriculum will be introduced to the pupils at the start of each academic year.

The Online Safety Charter will be prominently displayed in school classrooms, where the children have access to computers.

The key Online Safety advice will be promoted widely through school displays, newsletters, class activities and so on.

Incident Management

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Computing Co-ordinator and Deputy Head Teacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head Teacher.

An incident log will be kept to monitor what is happening and identify trends or specific concerns.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to Online Safety should be made to the ICT co-ordinator or Headteacher. Incidents must be logged and the **Flowcharts for Managing an Online Safety Incident** (see Appendix 2) should be followed.

Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Technician for recording, who will in turn, report to the Headteacher.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Technician and, depending on the seriousness of the offence, investigation by the Headteacher / Governors. This may result in immediate suspension, possibly leading to dismissal and involvement of police for very serious offences. Users are made aware of sanctions relating to the misuse or misconduct in line with the Code of Conduct.

Internet Access

The Internet is an open worldwide communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

INTERNET DOs AND DON'Ts:

DO:

- ✓ Use electronic services to promote effective teaching, learning and communication.
- ✓ Consider how the tone of emails may be perceived.
- ✓ Use appropriate language in emails, texts and appropriate social websites, which represents Boundary Primary School positively.
- ✓ Remember that digital mail and social websites may not be private.
- ✓ Ask the Head or Deputy Head teacher for ICT guidance if unsure or when needed.
- ✓ Cite references in emails for any facts that you present.
- ✓ Use approved, secure sources to enhance work life balance outside directed time e.g. ordering groceries, completing on-line forms such as motor tax or insurance.

DO NOT:

- ❖ **Allow children to use technological devices for internet access unsupervised**
- ❖ Access inappropriate material, nor save it to any School equipment, which may cause distress or offence
- ❖ Breach copyright laws by downloading or copying online material
- ❖ Use digital systems for activities which are not work related without the permission of the Headteacher
- ❖ Reveal any personal information (yours or other people's) electronically
- ❖ Assume attachments in messages are safe just because you know the sender
- ❖ Open unexpected attachments in emails
- ❖ Allow any volunteer or child, to access digital material unsupervised

Managing the Internet

The School provides pupils with supervised access to Internet resources (where reasonable) through the School's fixed and mobile Internet connectivity.

Staff will preview any recommended sites before use. Raw image searches are discouraged when working with pupils. Google Safe Search is recommended for all searches.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute School software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

Internet Use

Please also refer to the updated Code of Conduct.
You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.

Do not reveal names of colleagues, pupils, or any persons associated with the School; discuss School business or other confidential information acquired through your job on any social networking site or other online application.

On-line gambling or gaming is not allowed.
School internet access is controlled through Remedian IT Solutions' web filtering service.
Staff and pupils are aware that School based email and internet activity can be monitored and explored further if required.

Only designated staff have access to internet logs.

The School uses management control tools for controlling and monitoring workstations.

If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the Head Teacher or class teacher as appropriate.

Anti-virus protection is installed and kept up-to-date on all machines.

Please also refer to the Code of Conduct.

Managing Other Web Technologies

Please also refer to the Code of Conduct.
Online technologies, including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by **all** users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking to pupils within school premises.
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites, which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, e-mail address, specific hobbies / interests).
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of Cyber bullying to the School.
- Staff may only create blogs or other online media in order to communicate with pupils using the School website or other systems approved by the Headteacher.
- The school's Facebook page is monitored and updated by specific named members of staff. Updates on this page are for communicating key and essential messages as well as to celebrate and promote learning.

Parental Involvement

We believe that it is essential for parents / carers to be fully involved with promoting Online Safety both in and outside of School and to be aware of their responsibilities. We will regularly consult and discuss Online Safety with parents / carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Parents / carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on the school website).
All parents and carers are asked to sign a consent form allowing their child to be photographed or videoed while taking part in School activities, and for the image to be used within School.
This consent is assumed to roll forward from one year to the next, as long as the children remain on our School roll, unless told otherwise by the parent or carer. It allows School to take pictures of pupils engaged in educational activities such as sports events, drama productions, visits, etc., and to use these pictures internally and externally e.g. School web site.
This information is held on a central GDPR spreadsheet (on Google Drive) and can only be updated by 5 named members of staff. All staff in school **must** check this before uploading images to the website of Facebook page.

If parents/carers **do not** give consent, the child concerned will not have images taken of them.

All pictures taken will be appropriate, and will show children properly clothed for the activity they are engaged in. We do all we can to ensure that due sensitivity is shown in the choice and composition of images.

Parents / carers are expected to sign a **Home School agreement** containing the following statement:

We support Boundary's on-line safety education and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community.

Boundary Primary School disseminates information to parents relating to eSafety in the form of:

- Practical training sessions e.g. How to adjust the Facebook privacy settings
- Posters
- School website
- Newsletter items

There is an area on the school website dedicated to Online Safety which parents can access at any time for support.

Social Media

Please also refer to the Code of Conduct.
Facebook, Twitter and other forms of social media are increasingly becoming an important and popular part of daily life.

Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

Staff cannot set up social media accounts using their School email address. In order to be able to teach pupils the safe and responsible use of Facebook or other applications, ensure that you inform the Computing Co-ordinator if you are going to access these sites.

Pupils are not permitted to access their social media accounts whilst on school premises or an external visit organised by the school. **In line with KCSIE 2020, ‘we manage pupils’ use of their own devices’ children are not allowed to bring or use their own devices within school. Any devices brought into school will be locked in the school office for the day.**

Staff and governors should not name the School, reveal names of colleagues, pupils, or any persons associated with the school, discuss school business or disclose other confidential information acquired through your job on any social networking site or social media site.

Staff, governors, pupils, parents and carers are aware that their online behaviour must at all times be compatible with UK law.

PERSONAL AND PROFESSIONAL CONDUCT (from Teacher Standards 1.9.12)

A teacher is expected to demonstrate consistently high standards of personal and professional conduct. The following statements define the behaviour and attitudes, which set the required standard for conduct throughout a teacher’s career. Please ensure that you are complicit with the Code of Conduct and Teacher Standards.

Data Security

The management and appropriate use of Boundary School data is something that the School takes very seriously.

Security

The School gives relevant staff access to its Management Information Systems, with a unique username and password.

- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and will have read and signed the Acceptable use policy.

Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data.

Staff must avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight. Please see Acceptable Use Agreement.

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used. **This is line with GDPR guidance.**

Protective Marking

Appropriate labelling of data / media should help to secure data and so reduce the risk of security incidents.
Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business.
Applying too low a protective marking may lead to damaging consequences and compromise of the asset.
The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents.
□
We recommend 3 levels of labelling:
1. Unclassified (*or if unmarked*) – this will imply that the document contains no sensitive or personal information and will be a public document.
2. Protect – this should be the default setting and be applied to documents containing any sensitive or personal data. Marking documents as Protect will demonstrate an awareness of the Data Protection Act and Boundary’s responsibilities.
3. Restricted – documents containing any ultra sensitive data for even one person should be marked as Restricted.

Information Risk Owner (IRO)

The IRO is a member of staff who is familiar with information risks and the School's response and has the following responsibilities for information management:

owns the information risk policy and risk assessment.

appoints the Information Asset Owner(s) (IAOs).

acts as an advocate for information risk management.

Our school's IRO is Vicky Jones Boast (School Business Manager) and Suzanne Ashton (Headteacher).

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff, such as assessment records, medical information and special educational needs data. All such data should be assigned an Information Asset Owner, for example, the school's Management Information System (MIS) is the responsibility of the MIS Officer.

The role of an IAO is to understand:

what information is held, and for what purposes.

what information needs to be protected. How information will be amended or added to over time.

who has access to the data and why.

how information is retained and disposed of.

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

The IAO at Boundary is Vicky Jones Boast (School Business Manager), overseen by Suzanne Ashton (Head Teacher).

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Protecting Personal / Confidential Information

Ensure that any School information accessed from your own PC or removable media equipment is kept secure. Staff should not be accessing school information from personal equipment. In the event that they need to, staff are reminded to use their professional integrity, judgement and work inline with the Code of Conduct and Acceptable use policy. The School cannot monitor if staff secure data on personal devices.

Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.

Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.

Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.

Only download personal data from systems if expressly authorised to do so by your manager.

You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its' intended restricted audience.

Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

Remote Access

You are responsible for all activity via a remote access facility. This includes at home unmanaged devices that are not managed by the school. Only use equipment with an appropriate level of security for remote access.

To prevent unauthorised access to the School systems, keep all dial-up access information such as telephone numbers, login IDs and PINs confidential and do not disclose them to anyone.

Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers.

Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

There is additional guidance in relation to Remote Access in Appendix 4 of this policy for periods of school closure such as the period during the Covid-19 Pandemic in 2020.

Images and Film

Please also refer to the Code of Conduct.

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils **with School Equipment.**

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils. This includes when on field trips. **No School adult** will keep pupil's photographs or videos on any personal device / home computer.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others. **In line with KCSIE 2020, 'we manage pupils' use of their own devices' children are not allowed to bring or use their own devices within school. Any devices brought into school will be locked in the school office for the day.** Adults may bring mobile phones onto School premises, but must not use them to take photographs of children, or during the working hours of the school day.

We will not allow video and photographic recordings of performances by parents or other members of an audience, as this puts children at risk of having inappropriate images recorded of them, and the practicalities of monitoring this risk are too difficult for us to be able to ensure children's protection. Where there is sufficient demand for a recording, School will produce this itself, and make copies available, at cost price, to parents requesting them.

Only appropriate images and children's first names will be used on our website. Children will not be identified by their full name or address.

Permission to use images of all staff who work at Boundary is sought when necessary.

Children will be taught how to take pictures, and may photograph each other engaged in a range of learning activities. However, we will discourage them from taking close-up pictures of each other, and they will be supervised by an adult when they have access to a digital camera.

As soon as images have been used for their intended purpose, they will be deleted. School will not store digital images any longer than for their use in supporting pupils' learning during a particular piece of work.

Publishing

Media Publications:

Local or national media may visit School to follow up a news story, often to do with a notable achievement by a child or a group of children, for example, School may have raised money for a charity whose representative wants to receive the donation in person.

Where children's images might be made public, School will inform parents and carers of the event in advance, and allow them to withdraw their child from the event if they so wish. Media normally ask for the children's names to go alongside the photographs. If parents withhold consent for a child to appear in an event, then School will not allow the child to be involved.

On a child's entry to Boundary, all parents/carers will be asked to give permission to use their child's work/photos in the following ways: on the school web site; in the school prospectus and other printed publications that the school may produce for promotional purposes; recorded / transmitted on a video or webcam, in display material that may be used in the school's communal areas; in display material that may be used in external areas, i.e. exhibition promoting the school; general media appearances, e.g. local / national media / press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Webcams and CCTV

The School uses CCTV for security and safety. The only people with access to this are the SLT, Site Supervisor and ICT Support Manager. Notification of CCTV use is displayed at the front of the school.

We do not use publicly accessible webcams.

Webcams in the school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.

Misuse of the webcam by any member of the School community will result in sanctions, which could lead to disciplinary.

Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Videoconferencing

Permission is sought from parents and carers if their children are involved in video conferences.

Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.

All pupils are supervised by a member of staff when video conferencing.

All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.

The school keeps a record of video conferences, including date, time and participants.

Participants in conferences offered by 3rd party organisations may not be DBS checked. Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Videoconferences may be used between members of staff (not pupils) in times of school closure such as during the Covid-19 Pandemic in 2020. More information on this can be found in Appendix 4 of this policy.

ICT Equipment and Infrastructure

ICT Equipment

As a user of the School's ICT equipment, you are responsible for your activity.

The School logs ICT equipment issued to staff and records serial numbers as part of the inventory.

Do not allow your visitors to plug their ICT hardware into the School network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.

Ensure that all ICT equipment that you use is kept physically secure.

Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

It is imperative that you save your data on a frequent basis to the School network. You are responsible for the backup and restoration of any of your data that is not held on the school's network. Non-Sensitive data, e.g. planning, should only be stored on Google Drive. All other data should only be held on the school network.

Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted.

It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles. Personal images such not be used.

On termination of employment, resignation or transfer, return all ICT equipment to the School Business Manager. You must also provide details of all your system logons and passwords so that they can be disabled.

It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person. Please see AUA and Code of Conduct.

All ICT equipment allocated to staff must be authorised, by a member of the Senior Leadership team or those directed by the SLT.

Authorising mangers are responsible for: maintaining control of the allocation and transfer within their Unit and recovering and returning equipment when no longer needed.

All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Servers

Servers are kept in a locked and secure environment.

Access rights are limited.

The server is always password protected and locked, which only ICT technicians have access to.

Servers have security software installed appropriate to the machine’s specification.

Back up tapes are encrypted by appropriate software.

Data is backed up weekly.

Back up tapes are taken off site in a secure manner.

Remote back ups are automatically securely encrypted.

Portable Equipment

You are responsible for the security of your School portable device. Always set the PIN code and do not leave it unattended and on display (especially in vehicles).

Report the loss or theft of any Boundary mobile equipment immediately to the headteacher e.g. iPads, chrome books.

The School remains responsible for all call or data costs until a device is reported lost or stolen.

You must read and understand the user instructions and safety points relating to the use of your School mobile device prior to using it.

Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 111 emergency calls may be made if it would be unsafe to stop before doing so.

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using removable media, always consider if an alternative solution already exists. We have Google Drive so we should not need to use Removable hardware.

Only use recommended removable media. Encrypt and password protect.

In the event that you need to use removable media, it should be stored securely.

Removable media must be disposed of securely by the ICT support team in school.

Telephone Services

You may receive personal telephone calls from the telephone in office.
They are infrequent, kept as brief as possible and do not cause annoyance to others.
They are not for profit, to premium rate services or overseas.
They conform to this and other relevant School policies.

School telephones are provided specifically for School business purposes and personal usage is a privilege that will be withdrawn if abused.

Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

Ensure that your incoming telephone calls can be handled at all times.

Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your line manager.

Mobile Phones

Please also refer to the Code of Conduct.

Boundary Primary School are well aware that many primary-age children own a mobile phone and we understand the widespread growth in modern electronic communication. However, we are an institution that is primarily focused on learning and the safety and well-being of our pupils is paramount. **In line with KCSIE 2020, 'we manage pupils' use of their own devices' children are not allowed to bring or use their own devices within school. Any devices brought into school will be locked in the school office for the day.**

Mobile phones for children

The school policy is that children should not bring mobile phones or any form of electronic communication devices to school.

If a parent or guardian believes that there is a need for a child to be in possession of a mobile phone while at school they should write to the Headteacher to explain why this is so and why special dispensation should be allowed. The Headteacher will make a decision in all cases.

If a child is found in possession of a mobile phone it will be confiscated by a member of staff for the remainder of the school day and given to the school office for safe keeping. If this happens more than once the mobile will be returned to the parent or carer so that the school can explain why mobile phones are not permitted.

The school does not allow children to use mobile phones in school because:

- there are some concerns about the health risks connected to the frequent use of mobile phones.
- their use in school may distract pupils away from their work.
- mobile phones may be misused (for example, cyber bullying, viewing the Internet inappropriately and sending or receiving inappropriate images of members of the school community).
- staff time could be taken up investigating lost or even stolen mobile phones.

Should a child bring a mobile phone into school and report to an adult that they have been sent, exposed to or found access to indecent or obscene images/videos, the staff member should confiscate the phone and immediately pass it to SLT. They should not open or view any images, until advice has been sought from the police.

Mobile phones for staff

The School allows staff to bring in personal mobile phones for their own use.

During lesson times and in directed work time, personal mobile phones must be switched off or left on silent. Mobile phones should be stored in handbags, cupboards or lockers at all times when the adult is working with children and not kept on your person.

Mobile phones are not to be used when adults are working with children.

Staff should not use personal mobile phones to make or receive calls, text messages or emails during the working school day.

Mobile phones can only be used for private calls and text messages outside of a member of staff's working day (working day excludes lunchtime).

The sending of inappropriate or offensive text messages between any members of the school community is not permitted.

Disposal of Redundant ICT Equipment

All redundant ICT equipment will be disposed of through an authorised agency. This will 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 overwritten multiple times to ensure the data is irretrievably destroyed. 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 appropriate regulations.

The School maintains a comprehensive inventory of all its' ICT equipment including a record of disposal.

The School's disposal records 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 & / or / organisation who received the disposed item.
- Any redundant ICT equipment being considered for sale / gift will have been subject to an electrical safety check and hold a valid PAT certificate.

Writing and Reviewing this Policy

Staff, governors and pupils have been involved in making / reviewing the ICT Acceptable Use policies.

Review Procedure

There will be on-going opportunities for staff to discuss this policy or any issue that concerns them with the Headteacher.

There will be on-going opportunities for staff to discuss with the IRO/AIOs any issue of data security that concerns them.

This policy will be reviewed annually and consideration given to the implications for future of Boundary Primary Schools development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read and updated in June 2020.

Appendix 1 – Acceptable Use Agreement: Pupils.

Primary Pupil Acceptable Use Agreement / Online Safety Charter

We are ALL responsible for treating everyone online with respect. We will only use appropriate behaviour, language and images. We will only download or access content that is legal and does not breach copyright laws.

You have the right to:	You have the responsibility to:
enjoy the internet and all the fun and safe things it has to offer	use the internet sensibly, legally and not to harm others.
feel safe when using computers and modern technologies	use technologies legally and respectfully and to inform your teacher, if you encounter inappropriate, illegal or harmful content
be safe from bullying on the internet and the right to report it	treat others with respect and to report online bullying
explore the internet and to question any information you find	do this safely, sensibly and legally and to check any information before using it and use the websites that your teacher has stated.
keep information about you private and to only tell people what you want them to know about yourself	provide information that is not misleading, to keep your own data safe and not to misuse any information you have about others
decide whether or not you wish to communicate with someone, either online or through other digital technologies	be respectful when communicating with others electronically. You should always tell a responsible adult if something makes you feel uncomfortable or you become suspicious of another user's behaviour
choose whether to fill out forms or answer questions you find on the Internet	do this accurately and legally,
say **"NO!"** to being videoed or photographed by anyone using cameras, web cams, or mobile phones	protect yourself, by behaving in a way that will avoid embarrassment when videos and photographs are being taken
object to any videos or images of yourself being placed on the Internet, and to request that they are removed	use images and videos of yourself and others in a respectful and legal manner

Appendix 2 – Acceptable Use Agreement: Staff and Governors

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 staff and governors are aware of their professional responsibilities when using any form of ICT. All are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I understand that all digital activity must be appropriate to my professional activity, pupil's learning or approved positive work life balance activities outside directed time (e.g. on-line grocery ordering, motor car tax renewals). Access should only be made via authorised secure accounts and passwords, which should not be made available to any other person;
- I know that activity which threatens the integrity of School's or the Local Authority's ICT network, or activity that attacks or corrupts other systems, is forbidden;

- I know that use for personal financial gain, gambling, political purposes or advertising is forbidden;
- I know that posting anonymous messages and forwarding chain letters is forbidden;
- I know that using a mobile device for communication is forbidden during directed time, unless permission has been gained by either the Head or Deputy Headteacher previously
- I will educate the young people in my care in the safe use of ICT and embed Online Safety in my work with children and adults in my care.

For my professional and personal safety:

- I understand that School will monitor my use of the ICT systems, email and other digital communications
- I know that before I share any images with an audience, I must have the content approved by a member of the Senior Management Team, and never use an image of a prohibited child. See Designated Teacher or Child Protection Officer.
- I understand that the rules set out in this agreement also apply to use of School ICT systems and equipment (e.g. laptops, ipads, cameras, email, learning platform etc.) out of school;
- I understand that School ICT systems and equipment are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by Boundary Primary School.
- I know that if I use School equipment outside school for my personal use, I will not store any data on School equipment or network, nor will I access inappropriate material at any time using School equipment;
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher, Designated Teacher or Designated Officer.
- I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with School's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published e.g. on School's website, I will only use first names of those who are featured.
- I will not use social networking sites in School, using School equipment (unless I am a designated Boundary Facebook Administrator).
- I will not use social networking during my working hours.
- I will ensure that should I use a Facebook account (or similar social networking sites) that the account will be given strong privacy settings and that staff will be sensitive to the content of their publications. Photographs, comments or images should never refer to school life.

- I will only communicate with pupils, parents/carers using official School systems. Any such communication will be professional in tone and manner. I will not pass on my personal email addresses/mobile phones/social networking sites for such communications

- I will not engage in any online activity that may compromise my professional responsibilities
- When I use my School equipment (ipads/laptops/mobile phones etc.) in School, I will follow the rules set out in this agreement.
- I will ensure that any such devices are protected by up to date anti-virus software (F Secure), general updates and are free from viruses.
- I will not use personal email addresses on the School ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up following relevant School policies.
- I will not try to upload, download or access any materials which are illegal, inappropriate or open to question in a legal setting (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or may cause harm or distress to others.
- I will not try to bypass, or use any programmes or software that might allow me to bypass, the filtering/security systems in place to prevent access to such materials.
- I will not store, install or attempt to install programmes on any School or Local Authority equipment, nor will I try to alter computer settings, unless this is allowed in School policies
- I will not disable or cause damage to School equipment, or equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or School policy to disclose such information to an appropriate agency
- I will immediately report any damage or faults involving equipment or software, however this may have happened to the School office.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). I will use School accounts to purchase / gift resources in line with School practice. I will inform the ICT subject leader, Headteacher or Deputy Headteacher or School Business Manager before possible purchases.
- I understand that I am responsible for my actions in and out of School and that this AUP applies not only to my work and use of School ICT equipment in school, but also applies to my use of School ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by Boundary Primary School.
- I understand that if I fail to comply with this AUP or the Online Safety and Digital Data Policy, I could be subject to disciplinary action. This could include a warning: a suspension; referral to Governors and / or the Local Authority; and, in the event of illegal activities, the involvement of the Police.

<u>Further Guidance from Discussion at INSET:</u>

Social Website use outside directed hours:
Use minimal information on your homepage and a professional image which does not compromise your professionalism and integrity; If using School equipment outside the School, always supervise users to ensure compliance with this AUP; Ensure networking privacy settings are set to ‘friends only’, or their equivalent, and comply with standard requirements;
Never ‘friend’ a young person under the age of 16, who might compromise your integrity and professional status;
Before ‘tagging’ content, ensure that your professional integrity will not be compromised and that you have the subject’s permission.

Safeguarding Equipment and Data 12/11/18

- I understand that I should not transport confidential or personal data regarding the school or any member of the school community via pen drive or portable, removable usb.
- I understand that I should take all reasonable care with equipment that I am provided with (e.g. laptop, ipad, camera).
- I understand that I should ensure that equipment is left securely locked in the office within the school building, OR stored securely and out of sight off sight. e.g. not left in cars, not left in view of others.
- **I understand that in line with GDPR guidelines I should protect personal data to the best of my ability.**

I have read and understand the above and agree to use School ICT systems and equipment (both in and out of Boundary Primary School) and my own devices (in School and when carrying out communications related to School) within these guidelines.

Full name Post

Signed Date

Position:

Appendix 3 – Acceptable Use Agreement: Parents and Visitors

Acceptable Use Agreement / Code of Conduct

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 at Boundary Primary School This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff, parents and visitors are expected to are expected to respect the School's code of conduct and behave in an appropriate manner at all times. Any concerns or clarification should be discussed with the Headteacher.

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 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 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 or Governing Body. Personal or sensitive data taken off site must be encrypted.

I will not install any hardware of software without permission of the ICT technician.

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 and stored using School equipment and used for professional purposes 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 Headteacher.

I will support the School's 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.

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 Line Manager or the Headteacher.

I will respect copyright and intellectual property rights.

I will ensure that my online activity will not bring the School's into disrepute.

I will support and promote the School's Online Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

Name:

Signed:

Position/Visiting:

Appendix 4 – Additional measures and guidance for periods of School Closure

The following applies to periods of school closure such as the Covid-19 Pandemic in 2020 when in most cases, the majority of children will not be physically attending the school.

All staff who interact with children, including online, will continue to look out for signs a child may be at risk. Any such concerns are reported to the Designated Safeguarding Leader as soon as possible, and record through MyConcern, in line with the Prevent Policy.

When teaching online, the same principles as set out in Boundary's staff code of conduct policy are to be followed.

You are responsible for all activity via a remote access facility. This includes personal devices that are not managed by the school, when used for school purposes. Only use equipment with an appropriate level of security should be used for remote access. Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

An essential part of the online planning process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. As well as reporting routes back to the school. The safer internet page on Boundary School's website, signposts children to age appropriate practical support.

If a child raises a concern with you regarding their online safety, these should be reported to the DSL and recorded on MyConcern immediately. The computing coordinator can be contacted to provide support and advice.

If you have a concern about the security etc of any software used for remote teaching and learning, this should be raised immediately with the computing coordinator or ICT technician.

The communications that staff are having with parents/carers should be used to reinforce the importance of children being safe online. It is especially important for parents/carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school (if anyone) their child is going to be interacting with online.
Support for parents/carers to keep their children safe online includes:
Internet matters - for support for parents and carers to keep their children safe online
London Grid for Learning - for support for parents and carers to keep their children safe online
Net-aware - for support for parents and careers from the NSPCC
Parent info - for support for parents and carers to keep their children safe online
Thinkuknow - for advice from the National Crime Agency to stay safe online
UK Safer Internet Centre - advice for parents and carers
These support services are all shared on the Safer Internet part of the Boundary School website.

Videoconferencing may take place between members of staff during periods of such closures. These should only be held through secure and pre-approved software such as Google Meets. If alternative software wished to be used for a school purpose then permission must be sought from the computing coordinator or ICT technician. These meetings must remain professional in manner as per a meeting in school.

Online Safety Policy in brief

Boundary Primary School has an Acceptable Use policy, which is reviewed annually, and agreed by all staff. ICT Acceptable Use Agreements are signed by all staff, governors, students/visitors and pupils. Parents and visitors are made aware of the policy and the consequences of non-conformity.

Safe Handling of Data guidance documents are issued to all members of the school who have access to sensitive or personal data.

Protected and Restricted material must be encrypted if the material is to be removed from the School.

All servers are in lockable locations and managed by DBS-checked staff, under the control of the ICT Technician.

We use tape backup for the curriculum server, with an encrypted copy kept off-site. A secondary backup is created on NAS disks which are housed in a secure area.

The admin server is backed up at a 3rd party remote site using an encrypted service.

Disaster recovery of our admin server would use this remote backup service.

Disposal: Sensitive or personal material in electronic files is securely overwritten and other media shredded, incinerated or otherwise disintegrated when disposed of. We use accredited companies for the disposal of system hard drives where any protected or restricted data has been held.

Boundary paper-based sensitive information is shredded, using cross cut shredders, either on-site or under contract by a 3rd party company.

Laptops and iPads used by staff at home (loaned by the school) where used for any protected data are subject to the same policies as all other in-house ICT equipment, covering use of equipment, data security, etc.

Access to the setting-up of usernames and passwords which enable users to access data systems e.g. for email, network access, internet access is controlled by the ICT Support Manager.

Security policies are reviewed and staff updated at least annually.

Staff know how to report any incidents where data protection may have been compromised and have guidance documentation.

BlackpoolCouncil
BUILDING A BETTER COMMUNITY FOR ALL

Boundary Primary School's

Online Safety Charter

We are ALL responsible for treating everyone online with respect. We will only use appropriate behaviour, language and images. We will only download or access content that is legal and does not breach copyright laws.

You have the right to:	**You have the responsibility to:**
enjoy the internet and all the fun and safe things it has to offer	use the internet sensibly, legally and not to harm others.
feel safe when using computers and modern technologies	use technologies legally and respectfully and to inform relevant authorities, if you encounter inappropriate, illegal or harmful content
be safe from bullying on the internet and the right to report it	treat others with respect and to report online bullying
explore the internet and to question any information you find	do this safely, sensibly and legally and to check any information before using it and use the websites that your teacher has stated.
keep information about you private and to only tell people what you want them to know about yourself	provide information that is not misleading, to keep your own data safe and not to misuse any information you have about others
decide whether or not you wish to communicate with someone, either online or through other digital technologies	be respectful when communicating with others electronically. You should always tell a responsible adult if something makes you feel uncomfortable or you become suspicious of another user's behaviour
choose whether to fill out forms or answer questions you find on the Internet	do this accurately and legally
say **"NO!"** to being videoed or photographed by anyone using cameras, web cams, or mobile phones	protect yourself, by behaving in a way that will avoid embarrassment when videos and photographs are being taken
object to any videos or images of yourself being placed on the Internet, and to request that they are removed	use images and videos of yourself and others in a respectful and legal manner