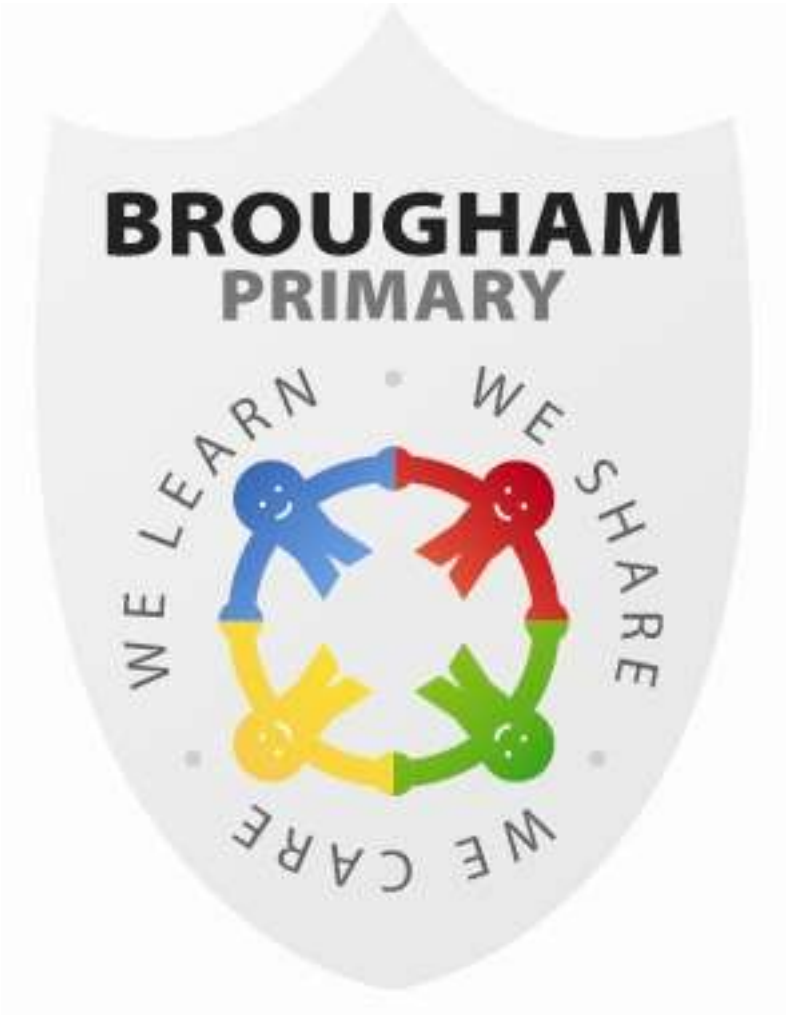

Policy for Information Governance (including Acceptable Use)

Policy Approved by Governors: **23.10.14**
Date for Review: **23.10.15**

Contents

1 Data Protection

1.1 Introduction

The processing of personal data by Brougham Primary School is essential to many of its services and functions. Compliance with the Data Protection Act 1998 ("the Act") will ensure that this processing is carried out fairly and lawfully. The Act seeks to strike a balance between, on the one hand, the needs of the organisation to function effectively and efficiently and, on the other, respect for the rights and freedoms of the individual. Brougham Primary School is committed to a policy of processing personal data within the law and ensuring that information about individuals is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

1.2 Data Protection Policy Statement

We, Brougham Primary School, will comply with all requirements of the Data Protection Act 1998. We will keep individuals informed of the purposes for which we are processing personal data, and will seek their consent where possible and appropriate. Where data is used for another purpose, individuals will be informed of this. We will also provide general information to the public on their rights under data protection legislation. We will hold the minimum personal data necessary to carry out the School's functions and every effort will be made to ensure its accuracy. Data which is no longer required will be securely destroyed. Processing will comply with the School's Information Governance Policies and will follow the Code of Practice contained in the standard ISO17779 (Information Security Management) where appropriate. We aim to respond to all requests from individuals to access their personal data within the timescales set down in the Data Protection Act 1998. Requests must be in writing, provide proof of ID, provide adequate information to be able to locate the data requested and be accompanied by the statutory maximum fee of £10. The Data Protection Act allows exemptions from subject access, providing information to Individuals and non-disclosure of information, in specific and limited circumstances. We will normally only invoke an exemption where it is deemed necessary to the effective operation of the School, for the prevention and detection of crime, to protect the individual, or is required by law. Governors and staff will be trained to an appropriate level in the use and control of personal data.

1.3 Definitions under the Data Protection Act 1998

In order to have an understanding of this policy it is important that the key definitions in the Act are understood.

1.4 Policy Scope

The policy applies to data that is;

- processed automatically by computer or other equipment capable of operating automatically in response to instructions or which is recorded with the intention of being so processed.

- recorded in structured and unstructured manual files.

1.5 Who it Concerns

4.1 This policy applies to all staff and members of the Governing body. As a matter of good practice, other agencies, partnerships and individuals working with the School, and who have access to personal data, will be expected to have read and complied with this policy. It is expected that staff who deal with external agencies will take responsibility for ensuring that such agencies sign an undertaking to abide by this policy.

1.6 Data Protection Principles

All processing of personal data must be done in accordance with the eight data protection principles.

Personal Data shall be processed fairly and lawfully. Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

The School will inform individuals of the purpose(s) for which it processes their personal data and will seek their consent where this is appropriate or required by law. Where data are used for further purposes the individuals will be informed of this.

Personal Data shall be adequate, relevant and not excessive in relation to the purpose for which it is held. Information, which is not strictly necessary for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

Personal Data shall be accurate and, where necessary, kept up to date. Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of the individuals to ensure that data held by the School are accurate and up-to-date and updated accordingly. It is the responsibility of the School to ensure that any notification regarding change of circumstances is noted and acted upon.

Personal Data shall be kept only for as long as necessary. The School will ensure that personal data are securely destroyed when no longer needed provided the retention periods required by law have been met.

Personal Data shall be processed in accordance with the rights of data subjects under the Data Protection Act. The School will respect the rights of individuals who are entitled:

- To ask the School if it holds personal information about them
- To ask what it uses the information for
- To be given a copy of the information (excluding any information exempt from disclosure under the Act)
- To be given details about the purposes for which the School uses the information and of other organisations or persons to whom it is disclosed.
- To ask for incorrect data to be corrected.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data. The School will

maintain procedures and provide training designed to ensure this principle is upheld through the organisation.

Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Data must not be transferred outside of the European Economic Area (EEA) – the twenty seven EU Member States together with Iceland, Liechtenstein and Norway – without the explicit consent of the individual. The School should be particularly aware of this when publishing Information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

1.7 Definitions Under the Data Protection Act

1.7.1 Personal Data

Personal data includes any information relating to a living individual who can be identified from the data either alone or in combination with other information relating to that person. This can include not only personal details, details of family and social circumstances, education, employment, business and financial details, but also goods or services received, expressions of opinions or intentions, and images such as those recorded on CCTV.

1.7.2 Sensitive Personal Data

The Act gives this category of personal data additional safeguards in relation to its processing. Sensitive personal data consist of information relation to;

- race or ethnic origin;
- political opinions;
- religious or similar beliefs;
- membership of trade unions;
- physical or mental health;
- sexual life;
- commission or alleged commission of any offence; or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

1.7.3 Processing of personal data

Processing is defined very widely in the Data Protection Act. The term processing includes obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data. It includes any of the following: organisation, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, alignment, combination, blocking, erasure or destruction. As such, most if not all operations involving personal data will be covered by the definition.

1.7.4 Data subject

A Data subject is any individual who is the subject of personal data. The definition excludes corporate entities, but will include individual employees and representatives of corporations.

1.7.5 Data Controller

A data controller is any person who determines the purposes for and the manner in which any personal data are or will be processed. Brougham Primary School is a data controller holding data on its employees and members of the public.

1.8 Security of Data

All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. Staff should form a judgement based upon the sensitivity of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access, or
- In a locked drawer or filing cabinet, or
- If computerised, password protected, or
- Kept on disks which are themselves kept securely

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as 'confidential waste'. Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff who process personal data at home. Offsite processing presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing personal data at home or in other locations outside the School.

1.9 Rights of Access to Data

Any individual who wishes to exercise this right should apply in writing to the Data Protection Officer. The School reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

In order to respond efficiently to subject access requests the School will have in place appropriate records management practices.

1.10 Retention and Disposal of Data

The School discourages the retention of personal data for longer than they are required.

Staff should regularly review files in accordance with the School's procedures on disposal and retention.

1.11 Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

1.12 Disclosure of Data

Personal data should only be disclosed to organisations or individuals specified in the School Notification to the Information Commissioner. The list of disclosures could include:

- School staff
- Elected members of the governing Body
- Other organisations (e.g. other local authorities, health authority). This includes organisations with whom we share and jointly manage personal data.
- Parents and guardians
- Data processors and their staff

All disclosures should be covered by written documentation, which should include details of the information to be disclosed, the reasons for the disclosure and the need for the recipient to comply with the Data Protection Act in handling the data. The documentation could be in the form of a data sharing agreement, a formal contract or a covering letter.
There may also be some instances where an organisation asks for disclosure of personal data about a specific individual, for example, in relation to a criminal investigation. Such requests must be in writing, and must specify what information is sought, for what purpose, and the legal powers under which the request is made.

1.13 Responsibilities

The School as a corporate body is the Data Controller under the Act.

The Data Protection Officer. The Data Protection Officer is responsible for day to day data protection matters and for developing specific guidance notes on data protection issues. At Brougham Primary School this is the responsibility of the Head Teacher.

Staff/Governors and third parties. Compliance with data protection legislation is the responsibility of all staff, members of the Governing body and third parties with access to personal data held by the School.

Information Governance Group. A Local Authority convened group has been established to develop and implement appropriate policies and procedures for information governance and as such will be an appropriate forum for sharing best practice and seeking advice in relation to information governance.

The Head Teacher is responsible for reviewing this policy and related policies and procedures on information governance.

1.14 Notification

Brougham Primary School must notify the information commissioner of all personal data being processed which is subject to the Act.

Notification is the responsibility of the Data Protection Officer. Details of the Brougham Primary School Notification are published on the Information Commissioner's website www.ico.gov.uk. Anyone who is, or intends, processing data for purposes not included in the School's Notification should seek advice from the Data Protection Officer.

1.15 Implementation

13.1 The policy will be relayed to new employees as part of the induction process. The Data Protection Officer will inform existing employees. This policy will be published on the Schools shared area and updated accordingly.

1.16 Monitoring and Review

14.1 This policy will be monitored by the Data Protection Officer, and will be reviewed annually to ensure that it remains up to date and relevant.

1.17 Relation Legislation, Standards and Policies

1.17.1 Main Legislation

- Freedom of information Act 2000 (providing overarching right of access to all information held by a public authority).
- Human Rights Act 1998 (brings much of European Convention on Human Rights into UK law).

1.17.2 Professional Standards

- BS4783 Storage, transportation and maintenance of media for use in data processing and information storage.
- ISO 17799 Standard on Information Security Management.
- ISO 15489 Standard on Best Practice in Records Management.
- BSI DISC PD 0008:1999 Code of practice for legal admissibility and evidential weight of information stored electronically.
- BSI DISC PD 0010:1997 the principles of good practice for information management.
- BSI DISC PD 0012: Guide to the practical implications of the Data Protection Act.

2 Email

Brougham Primary School will ensure all users of the email facilities are aware of the acceptable use of such facilities.

2.1 Purpose

The objective of this section of the information governance policy is to direct all users of the School's email facilities by:

- Providing guidance on expected working practice.
- Highlighting issues affecting the use of email.
- Informing users about the acceptable use of ICT facilities in relation to emails.
- Describing the standards that users must maintain.

- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

This section establishes a framework within which users of the School's email facilities can apply self-regulation to their use of email as a communication and recording tool.

2.2 Scope

This section covers all email systems and facilities that are provided by Brougham Primary School for the purpose of conducting and supporting official business activity through the School's network infrastructure and all stand alone and portable computer devices.

This policy is intended for all Brougham Primary School employees, contractual third parties and agents of the School who have been designated as authorised users of email facilities.

The use of email facilities will be permitted only by staff that have been specifically designated as authorised users for that purpose, and have confirmed in writing that they accept and agree to abide by the terms of this policy.

The use of email facilities by staff that have not been authorised for that purpose will be regarded as a disciplinary offence.

2.3 Definition

All email prepared and sent from Brougham Primary School email addresses or mailboxes, and any non-work email sent using Brougham Primary School ICT facilities is subject to this policy.

2.4 Risks

Brougham Primary School recognises that there are risks associated with users accessing and handling information in order to conduct official School business.

This policy aims to mitigate the following risks:

- Failure to report information security incidents
- Inadequate destruction of data
- Loss of direct control of user access to information systems
- Exposure to legal action and / or adverse publicity
- Time wasting by inappropriate and unauthorised use
- Incorrect handling of confidential information see below

If there any questions or doubts about which category the information you are dealing with falls into then you should contact Gillian Sild.

Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and an inability to provide necessary services to our customers**.**

2.5 Applying the Policy

2.5.1 Email as Records

All emails that are used to conduct or support official Brougham Primary School business must be sent using a (brougham.hartlepool.sch.uk) or "@hartlepool.gov.uk" address.

Non-work email accounts **must not** be used to conduct or support Brougham Primary School business. Users must ensure that any emails containing sensitive information must be sent from an official School email (gov.uk). Any emails containing confidential information must be marked as such and when being sent externally, sent using WinZip encryption or via another approved encrypted means. All emails that represent aspects of Brougham Primary School business are the property of Brougham Primary School and not of any individual employee.

Users should be aware any emails and attachments may need to be disclosed under the Data Protection Act or the Freedom of Information Act.

Emails held on the School's equipment are considered to be part of the corporate record and email also provides a record of staff activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any email message sent from a facility provided to conduct or support official Brougham Primary School business should be considered to be an official communication from the School. In order to ensure that Brougham Primary School is protected adequately from misuse of e-mail, the following controls will be exercised:

- It is a condition of acceptance of this policy that users comply with the instructions given in this policy. Users who need further advice and guidance should contact the E safety officer.

- All official external e-mail must carry the following disclaimer:

  This document is strictly confidential and is intended only for use by the addressee. If you are not the intended recipient, any disclosure, copying, distribution or other action taken in reliance of the information contained in this email is strictly prohibited.
  Any views expressed by the sender of this message are not necessarily those of Brougham Primary School. If you have received this transmission in error, please use the reply function to tell us and then permanently delete what you have received.

  Please note: Incoming and outgoing e-mail messages are routinely monitored for compliance with our policy on the use of electronic communications.

- External email Signatures must follow the School standard and contain the following details:-

  Name
  Post Title
  School Name
  Address
  Telephone number
  Fax Number
  Email Address

Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the School's ICT systems.

It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the School Administrator or E Safety officer.

2.5.2 Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, or that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or confidential information or of communicating in the particular circumstances.

All emails sent to conduct or support official Brougham Primary School business must comply with School communications standards.

Email must not be considered to be any less formal than memos or letters that are sent out. When sending external email, care should be taken not to contain any material which would reflect poorly on the School's reputation or its relationship with parents/pupils, clients or business partners.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the School's Equality Policy, or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any material, should consult the E Safety officer prior to commencing any associated activity or process.

IT facilities provided by the School for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of confidential material concerning the activities of the School.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.

- For so-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For disclosing to others any information given in a document classified with a protective marking without the prior consent of a person authorised to give it, unless under a requirement of law.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the School into disrepute.
- Printing off large volumes of personal emails and/or attachments using work printers unless arrangements have been made to reimburse the cost to the School.
- Reading lengthy incoming personal emails and/or attachments during working hours.
- Drafting and/or sending an unreasonable amount of outgoing personal emails during working hours.

2.5.3 Acceptable use of the School e-mail facility and addresses includes

- Receiving small numbers of personal emails
- Printing off the occasional personal email and/or attachment using work printers
- Opening and identifying an email as being personal (once recognised as being personal the remainder of the email should not be read during working hours unless it is very short)
- Reading lengthy incoming personal emails and/or attachments outside of working hours
- Drafting and/or sending outgoing personal emails and/or attachments outside of working hours

Personal emails using School facilities are subject to the same conditions as business use. Further guidance on what is acceptable and unacceptable use contact the E Safety officer.

2.5.4 Junk Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter emails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using Brougham Primary School systems or facilities.

2.5.5 Categorisation of Messages

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. It is advisable that all emails are protectively marked with confidential unless they are free to circulate publicly.

2.5.6 Security

Emails sent between brougham.hartlepool.sch.uk addresses are held with the same network and are deemed to be secure. All emails travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, confidential material must not be sent via email outside this closed network, unless encryption is used.

2.5.7 Confidentiality

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If any member of staff is unsure about whether they should pass on information, they should consult the Headteacher.

Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of Brougham Primary School.

Care should be taken when addressing all emails, but particularly where they include confidential information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent confidential material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the Gillian Sild.

2.5.8 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of Brougham's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to the ICT Technician.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access School facilities.
- Must report any suspected files to the ICT Technician.

In addition, the School will ensure that email is virus checked using the anti-virus software.

If a computer virus is transmitted to another organisation, the School could be held liable if there has been negligence in allowing the virus to be transmitted.

2.5.9 Accessing Emails using Outlook Web Access

Currently, in order to access Brougham Primary School email accounts remotely, the following actions are necessary (whether it be on a computer or Smartphone):

1. Sign in to Remote access
2. enter username and password
3. read emails

There are now apps for Smartphones that will automate the steps above.

Effectively this means that the only security in place on Smartphones to prevent unauthorised access to Brougham Primary School email if this app is used with a 4 digit pin or password on the phone (provided one has been set up). For clarity, this means that if your phone is stolen, misplaced etc. and not locked, anyone would potentially have access to your email account and everything it contains.

All staff are therefore instructed that anyone accessing School emails on Smartphones **must setup a pin code security.**

2.5.10 Whom Should I Ask if I Have Any Questions?

This policy will be publicised and made available to all users on the School's website.

In addition all new School email (and internet) users must certify to say they have read, understood and accept the terms of use as set out in this policy (see Acceptable use section).

Should employees have any questions regarding Internet use or about any aspects of the policy they should, in the first instance, refer them to the Headteacher, School Business Manager and/or ICT Technician.

2.6 Policy Compliance

If any user is found to have breached this policy, they may be subject to Brougham Primary School's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Headteacher.

2.7 Key Messages

- All emails that are used to conduct or support official Brougham Primary School business must be sent using a brougham@school.hartlepool.gov.uk or brougham.hartlepool.sch.uk
- Non-work email accounts **must not** be used to conduct or support official Brougham Primary School business.
- Users must ensure that any emails containing sensitive information must be sent from an official School email.
- All official external email must carry the official Brougham Primary School disclaimer

- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the School's Equality policy.
- Automatic forwarding of email must be considered carefully to prevent material being forwarded inappropriately.
- Email should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Anonymous messages and chain letters must not be sent.
- Email attachments should only be opened if the source is known and trusted.
- Pupils are not permitted under any circumstances to email a member of staff's personal email address. Specific pupil/teacher email accounts are provided for this purpose.
- Users must ensure that all necessary steps are taken to protect confidential emails. The School will be liable for any defamatory information circulated either within the School or to external contacts.
- The school email system and accounts must never be registered or subscribed to SPAM.
- Any unsuitable emails received must be reported to the E Safety Officer
- Offers or contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between you or the school and the recipient. Never commit the school to any obligations by email or the internet without ensuring that you have the authority to do so. If you have any concerns contact the Head teacher.
- Employee use of personal email accounts is only permitted if the equipment on which it is accessed has built-in anti-virus protection approved by the school. Access to your personal email is allowed during break/lunch times provided it does not interfere with your school related responsibilities and does not contravene the ICT usage rules outlined in this document or other policy documentation.

3 Remote Access

3.1 Policy Statement

Brougham Primary School provides users with the facilities and opportunities to work remotely as appropriate to their role. Brougham Primary School will ensure that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.

3.2 Purpose

The purpose of this document is to state the Remote Working policy of Brougham Primary School.

Portable computing devices are provided to assist users to conduct official School business efficiently and effectively. This equipment, and any information stored on portable computing devices, should be recognised as valuable organisational information assets and safeguarded appropriately.

3.3 Scope

This document applies to all employees, contractual third parties and agents of the School who use/access Brougham Primary School ICT facilities and equipment remotely, or who require remote access to Brougham Primary School Information Systems or information.

3.4 Definition

This policy should be adhered to at all times whenever any user makes use of portable computing devices. This policy applies to all users' use of Brougham Primary School ICT equipment and personal ICT equipment when working on official School business away from Brougham Primary School premises (i.e. working remotely).

This policy also applies to all users' use of Brougham Primary School ICT equipment and personal ICT equipment to access School information systems or information whilst outside the United Kingdom.

Portable computing devices include, but are not restricted to, the following:

- Laptop computers.
- Tablet PCs.
- PDAs.
- Mobile phones.
- Text pagers.
- Wireless technologies.

3.5 Risks

Brougham Primary School recognises that there are risks associated with users accessing and handling information in order to conduct official School business. The mobility, technology and information that make portable computing devices so useful to employees and organisations also make them valuable prizes for thieves. Securing confidential information when users work remotely or beyond the School network is a pressing issue – particularly in relation to the School's need as an organisation to protect data in line with the requirements of the Data Protection Act 1998.

This section aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft.
- Wider use of mobile IT equipment where personal or sensitive data may be stored.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to confidential information.
- Exposure of personal and sensitive client information.
- Unauthorised introduction of malicious software and viruses.
- Potential sanctions against the School or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the School or individuals as a result of information loss or misuse.
- School reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and an inability to provide necessary services to our customers, as well as exposing sensitive and/or personal client data to unauthorised users/environments.

3.6 Applying the Policy

All ICT equipment (including portable computer devices) supplied to users is the property of Brougham Primary School. It must be returned upon the request of Brougham Primary School. Access for the ICT Technician. of Brougham Primary School shall be given to allow essential maintenance, security work or removal upon request.

All ICT equipment will be supplied and installed by the Brougham Primary School ICT Technician. Hardware and software **must only** be installed following approval by Brougham Primary School. Users who wish to install any hardware or software must contact the ICT Technician before this is carried out.

3.7 User Responsibility

It is the user's responsibility to ensure that the following points are adhered to at all times:

a) Users must take due care and attention of portable computer devices when moving between home and another business site.

b) Users will not install any hardware to or inside any School owned portable computer device, unless authorised by Brougham Primary School ICT Technician.

c) Users will allow the installation and maintenance of Brougham Primary School installed Anti Virus updates immediately.

d) Users will inform the ICT Technician. of any School owned portable computer device message relating to configuration changes.

e) Business critical data should be stored on the school server wherever possible and not held on the portable computer device. Confidential information should be saved in the staff private folder and not in shared folders.

f) All mobile devices (e.g. laptops and tablet PC's) must be locked with a password/PIN number.

g) Personal, sensitive or confidential documents can only be stored on either a school issued encrypted USB drive or in the encrypted folder on the school issued laptop.

h) Any personal or sensitive documents saved temporarily in the above locations must be copied to the School network and then removed from the hard drive as soon as you can access the network. Personal or sensitive documents must not be allowed to remain on mobile devices.

i) If you take a school laptop home with you, it should be stored in a secure location and you must make sure that it is not left in your car etc.

j) All faults must be reported to the IT Technician immediately.

k) Users must not remove or deface any asset registration number and only those devices with an asset number/tag can be connected to the School network.

l) User requests for upgrades of hardware or software must be approved by the ICT Technician and leader. Equipment and software will then be purchased and installed by ICT Technician.

m) Personal use of the ICT equipment by staff is allowed outside of working hours. However this policy and acceptable use must be fully adhered to. In particular, the equipment must not be used in relation to running an external business and websites

containing illegal, unsuitable and inappropriate material, must not be accessed. Only software approved by Brougham Primary Scholl can be used (e.g. Word, Excel, Adobe, etc.). The ICT equipment is supplied for the employee's sole use and nobody else, including family members, must use it.

n) The user must ensure that reasonable care is taken of the ICT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, Brougham Primary School may recover the costs of repair (calculated at a pre-determined rate). This charge is subject to annual review.

o) The user should seek advice from the Headteacher before taking any School supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the School's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel.

p) Brougham Primary School may at any time, and without notice, request a software or hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

q) Any user who chooses to undertake work at home or remotely in relation to their official duties using <u>their own</u> IT equipment must understand that they are not permitted to hold any database, or carry out any processing of confidential information relating to the School, its employees, or pupils/parents. **Under no circumstances** should personal or confidential information be emailed to a private non-School email address. For further information, please refer to the School Email section of this policy.

3.8 <u>Remote and Mobile Working Arrangements</u>

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that where possible the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use, e.g. put away in cupboard, locked in cabinet etc.

Users must ensure that passwords are kept in a separate location to the portable computer device at all times. All removable media devices and paper documentation must also not be stored with the portable computer device. Passwords and/or other access information should not be written down and stored near the portable device.

Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Where personal and sensitive information is being printed on shared printers extreme care should be taken to ensure **all** documents are collected from the printer and that interruptions to printing due to paper jams, empty paper trays etc do not lead to sensitive documents being discovered by unauthorised staff.
Waste paper containing confidential information must be shredded to required standards. If paper documents containing sensitive information are taken outside the office, the number of documents/cases should be limited in the same was as electronic records.

3.9 Access Controls

It is essential that access to all confidential information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must be encrypted. If this is not possible, then all confidential data held on the portable device must be encrypted. It is School policy to encrypt/lock all laptops.

Remote users' access to School systems (if connecting over public networks, such as the Internet) will need to be via a secure route. No other access routes can be used.

The user shall ensure that appropriate security measures are taken to stop unauthorized access to confidential information, either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as Brougham Primary School itself.

3.10 Anti Virus Protection

The ICT Technician. through Brougham Primary School will deploy an up-to-date Anti Virus signature file to all users who work away from the Brougham Primary School premises. Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least once every week (unless valid reasons why this cannot be achieved, e.g. sickness) to enable the Anti Virus software to be updated.

3.11 Policy Compliance

If any user is found to have breached this policy, they may be subject to Brougham Primary School's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Headteacher.

3.12 Key Messages

- Users must familiarise themselves with the detail of this policy before embarking on remote working.
- It is the user's responsibility to use portable computer devices in an acceptable way. This includes not installing software that has not been approved, taking due care and attention when transporting and storing the equipment and not emailing confidential information to a non-School email address.
- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- It is the user's responsibility to ensure that access to all confidential information is controlled e.g. through password controls.

- All confidential data held on portable computer devices must be encrypted.
- If any user has any doubt as to what is or is not acceptable use of mobile devices, they should contact the Headteacher.

4 Removable Media

Brougham Primary School will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and ICT equipment for the purposes of conducting official School business.

4.1 Purpose

This section states the Removable Media policy for Brougham Primary School. The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of Brougham Primary School's computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Protected and Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

4.2 Scope

This policy applies to all employees, contractual third parties and agents of the School who have access to Brougham Primary School information, information systems or ICT equipment and intend to store any information on removable media devices.

4.3 Definition

This policy should be adhered to at all times, but specifically whenever any user intends to store information used by the School to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

4.4 Risks

Brougham Primary School recognises that there are risks associated with users accessing and handling information in order to conduct official School business. Information is used throughout the School and sometimes shared with external organisations and applicants. Securing confidential data is of paramount importance – particularly in relation to the School's need to protect data in line with the requirements of the Data Protection Act 1998.

Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the School. It is therefore essential for the continued operation of the School that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the School's needs.

This policy aims to mitigate the following risks:

- Disclosure of confidential information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of School networks or equipment through the introduction of viruses through the transfer of data from one form of ICT equipment to another.
- Potential sanctions against the School or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the School or individuals as a result of information loss or misuse.
- School reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and an inability to provide necessary services to our pupils/parents.

4.5 Applying the Policy

4.5.1 Procurement of Removable Media

All USB memory sticks and external hard drive devices must be procured by the school and have encryption activated on them and **must only** be used with School owned ICT equipment.

4.5.2 Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment, than data which is frequently backed up. Therefore removable media should not be the only place where data obtained for School purposes is held. Copies of any data stored on removable media must also remain on the source system or network until the data is successfully transferred back to the network or system. Data stored on removable media must only be done so temporarily and removed at the earliest opportunity. Data should not be permanently held on a removable media device.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media, must be stored on encrypted removable media devices.

4.5.3 Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to the Headteacher.

4.5.4 Third Party Access to School Information

No third party (external contractors, partners, agents, the public or non-employee parties) may extract information from the School network information stores or ICT equipment and place on a removable media device without explicit agreement by the Headteacher following advice from the ICT Technician and E Safety Officer.

Should third parties be allowed access to School information then all the considerations of this policy apply to their storing and transferring of the data.

4.5.5 Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to stop using removable media when it is damaged.

Virus and malware checking software approved by the School must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded.

Whilst in transit or storage the data held must be on an encrypted device to reduce risk to the School, other organisations or individuals from the data being lost whilst in transit or storage.

4.5.6 Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to the ICT Technician for disposal.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the ICT Technician.

4.5.7 User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs:

- Any removable media device used in connection with School equipment or the network or to hold information used to conduct official School business **must** be checked for viruses/malware before use.
- All data stored on removable media devices **must** only be stored on encrypted devices.

- Virus and malware checking software **must** be used when the removable media device is connected to a machine.

- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.

- Removable media devices **must not** to be used for archiving or storing records as an alternative to other storage equipment.

- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

- A record of the information placed onto any removable media device **must** be kept by the user and be available to the School.

- Information held on a removable media device must be kept to a minimum.

- All information should be removed from the removable media device and placed onto the School networked system as soon as available.

For advice or assistance on how to securely use removable media devices, or for further advice or clarification on any part of this policy, please contact the ICT Technician.

4.6 Policy Compliance

Whilst respecting the privacy of authorised users, Brougham Primary School maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of removable media by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of items from removable media does not necessarily result in permanent deletion.

In addition to routine monitoring and audits, where a member of staff suspects that the removable media is being abused or misused by a user, they should inform the Head Teacher or E Safety Officer. Should an investigation be authorised, designated staff may carry out an Internal Audit.

In addition the School will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for information.

If any user is found to have breached this policy, they may be subject to Brougham Primary School's disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Head Teacher.

4.7 Key Messages

The key messages within this policy are summarised below:-

- Any removable media device used for confidential data **must be** encrypted.
- Damaged or faulty removable media devices must not be used to store confidential data.

- Special care **must be** taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage.

5 ICT Acceptable Use

5.1 Introduction

The Governing Body of Brougham Primary School is committed to ensuring that all employees, pupils and other users are aware of their responsibilities regarding use of school ICT equipment, software, and ICT network.

Responsibility for this policy rests with the Governing Body and Head teacher. It applies to all users of the school ICT systems including 'Guests'.

The use of ICT facilities within the school is encouraged, as its appropriate use facilitates communication and can improve efficiency. Used correctly, it is a tool that is of assistance to employees and pupils. Inappropriate use, however, causes many problems, ranging from minor distractions to exposing the school to financial, technical, commercial and legal risks.

Our Acceptable Use policy has been created to ensure the school network is operated safely and all users of ICT are safe. It refers to our school ICT network and to the use of equipment and mobile technologies within it, and outlines the behaviours which are acceptable and unacceptable within our school.

Our Acceptable Use policy must be fully complied with by users at all times. It should be noted that the school network is monitored on a regular basis. Any person who is found to have misused the school system or not followed our policy could face the following consequences;

- Temporary or permanent withdrawal from the school system
- Suspension or exclusion from the school
- Disciplinary action
- In the most serious cases legal action may also be taken.

5.2 Network Protocol

- The school network and associated services may be used for lawful purposes only.
- School network and internet use must be appropriate to a pupil's education or to employee professional activity. If unsure about your required use, please seek authorisation from the Head teacher or E Safety Officer.
- Users must respect other people's work/material and must not interfere with it.
- Users must not misuse or waste ICT resources, particularly printer ink, toner and paper and network traffic (e.g. sending lots of printing to a printer).
- Employees may use ICT facilities for personal use during break/lunch times provided it does not interfere with their school related responsibilities and does not contravene the ICT usage rules outlined in this document.
- Users must not copy, record or distribute any material from or with the school network facilities that may be illegal to do so. This can include television media, films, telephone

conversations and music. If you are unsure if you have permission to do so please see the School administrator.

- Use of the school network will be supervised by key logging security software and will monitor all activity, recording any inappropriate language or use, e.g. chat rooms, internet use, typing and file names etc.
- The E Safety officer can remotely view or interact with any of the computers on the school network. This may be used randomly to implement the ICT Policy and to assist with any user difficulties.
- Users must ensure that confidential employee/pupil related information is not stored within school shared areas.
- Users should ensure their files/folders are structured within their account in an efficient manner to utilise space on the school network.

5.3 Passwords

- Each pupil from year one onwards working within the school must log on using their own name or initials and their own password and log off at the end of the session. This will be set up taking into consideration the capability of the child and in minimising the negative impact on teaching and learning within the classroom.
- Each employee must log on using their own user name and password. When equipment is left unattended, you must log off or a password protected screen saver must be activated.
- Any supply teachers or visitors to the school must log onto the system as a Guest only and a record will be kept by the School Administratror who is using each unique Guest password.
- Pupils, employees or visitors must not give their password or user account details to anyone. This comes under the Computer Misuse Act and is illegal. If your password is lost or someone discovers your password you must inform the Headteacher.
- All users must not attempt to use someone else's network account.
- Passwords must be changed at regular intervals.

5.4 Hardware, Software and Downloads

- Users must not install hardware devices onto the network without permission from ICT Technician.
- Users of the network must virus check any USB device or storage device before using it on the network.
- Users must not install software onto the network from a CD-ROM, other device or by downloading from the Internet without permission from the ICT Technician.
- Copyright and intellectual property rights must be respected when downloading from the internet.
- Users must not attempt to use the School's ICT facilities to undertake any form of piracy including the infringement of software licences or other copyright provisions whether knowingly or not. This is illegal.
- Users must not purchase any ICT facilities without the consent of the ICT Technician., ICT leader or Head teacher. This is in addition to any purchasing arrangements followed according to school policy.
- Users must not knowingly distribute or introduce a virus or harmful code onto the school's network or equipment. Doing so could lead to action by the school outlined in the introduction.
- Users must not relocate, take off-site or otherwise interfere with the ICT facilities without the authorisation of the Headteacher, School Business Manager or ICT Technician.

- If employees wish to book out ICT equipment for use away from school premises (with the exception of school staff laptops which are already logged) please see the Headteacher, School Business Manager or ICT Technician.
- Users must not misuse or damage ICT related equipment.

5.5 Images/videos

- All pupils may have photographs taken or videos made in line with school requirements unless parents indicate they do not wish it.
- Photos or videos which include nudity or inappropriate actions are not permitted to be taken, downloaded, viewed or stored under any circumstance on school ICT equipment or the network.
- All images and videos will be analysed by school security software. If there is a suspicion they are inappropriate they will be recorded for nominated staff to review and take action if necessary.
- Images of pupils should not be posted on personal social networking sites.

5.6 Internet Usage

- Pupils must be supervised at all times when using the internet.
- Use of all internet sites will be recorded and analysed for nominated staff to review and take action if necessary.
- Use of the internet for personal financial gain, gambling, political purposes, advertising or illegal activity is forbidden.

5.7 Internal Phone/Postal System

- Telephone and postal system use must be appropriate to a pupil's education or to staff professional activity. If you are unsure about your required use, please seek authorisation from your line manager or the Headteacher or School administrator.
- Staff use of the school's telephone facilities for personal use is permitted for necessary UK calls lasting less than 10 minutes so long as this does not interfere with your job role duties. If you need to use the telephone for longer than this or you need to make a call overseas, authorisation must be sought first from the Head teacher and authorisation must be requested on each occasion. However, the Head teacher or School administrator should be notified immediately after the call. Any personal use of the telephones is at the Head teacher's discretion and should fall within reasonable usage.
- Users must not re-locate, take off-site or otherwise interfere with the telephone system facilities without the authorisation of the Headteacher.
- Users must not utilise the school phone/post facilities to access, receive, view or display any of the following;

    - Any material that is illegal.
    - Any material that could constitute bullying or harassment or any negative comment about other persons or organisations.
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false.
    - Any sexually explicit material.
    - Any adult or chat-line phone numbers.

- All users are prohibited from attempting to use the school's phone/post facilities to undertake ANY form of piracy including the infringement of media rights or other copyright provisions whether knowingly or not. This is illegal.
- Users must not copy, record or distribute any material from or with the school phone/post facilities that may be illegal to do so. This can include television media, films, telephone conversations and music. If you are unsure if you have permission to do this please see the Head Teacher or school administrator.

5.8 Mobile devices

- Employee personal mobile phones/devices must not be connected to the school data/internet network but can be connected to the Guest internet connection.
- Employees are advised to security lock their mobile phones when left unattended.
- Images of pupils should not be stored on any personal mobile device. Images taken using school mobile devices must not be removed from school premises without authorisation from the Head teacher.
- Employees who are allocated a school mobile device and are authorised to take the device home must ensure they have adequate cover on their home insurance to provide a replacement if the device is damaged in an accident or stolen.
- Any personal use of mobile devices is at the Head teacher's discretion and should fall within reasonable usage.

5.9 Social Networking

All users must comply with the specific guidance and instructions set out in the Local Authority Social Networking policy that has been approved by the Governing Body for all staff working at Brougham Primary School.

5.10 School Email, Removable Media and Remote Access

All users must comply with the specific guidance and instructions set out in the respective sections of this policy (above).

5.11 Reporting Incidents

- Employees are required to inform the Head teacher or E Safety Officer immediately of any abuse of the school ICT systems.
- Pupils are required to inform a member of staff immediately of any abuse of the school ICT systems.

6 ICT Acceptable Use Assurance Statement

I have read, understood and agree to comply with the school Information Governance and Acceptable Use Policy issued to me.

Signed: .....

Print Name: .....

Date: .....

Print name: .....