Bowesfield
Primary School

Online Safety Policy 2020

Date approved by Governing Body: 30.11.20.
Review Date: October 2021

Bowesfield Primary School Online Safety Policy

Article 3 (best interests of the child) The best interests of the child must be a top priority in all decisions and actions that affect children.

Article 13 (freedom of expression) Every child must be free to express their thoughts and opinions and to access all kinds of information, as long as it is within the law

Article 15 (freedom of association) Every child has the right to meet with other children and to join groups and organisations, as long as this does not stop other people from enjoying their rights.

Article 16 (right to privacy) Every child has the right to privacy. The law should protect the child's private, family and home life, including protecting children from unlawful attacks that harm their reputation.

Article 17 (access to information from the media) Every child has the right to reliable information from a variety of sources, and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them.

Article 31 (leisure, play and culture) Every child has the right to relax, play and take part in a wide range of cultural and artistic activities.

Introduction

Access to online technology has become an essential part of everyday life, both in and out of school. As well as supporting teaching and learning; many members of our school community enjoy use of a number of online technologies such as:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Apps

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

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Roles and responsibilities

The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The governor who oversees safeguarding, including online safety is Janet Marriott.

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

The designated safeguarding lead

Details of the school's designated safeguarding lead/deputies (Emily Hodgeon, Claire Cotterill, Jo Vollands-Ross and Charlotte Hardiman) are set out in our child protection policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the computing lead, ICT manager and other staff, as necessary, to address any online safety issues or incidents

Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's anti-bullying policy

Liaising with other agencies and/or external services if necessary

The computing lead

The computing lead (Louise Hadfield) will support the DSL by:

Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Maintaining an up to date list of staff and pupils who have/have not completed the acceptable use policy

Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's anti-bullying policy

Working with the ICT manager to ensure ICT systems are secure and updated regularly

Liaising with other agencies and/or external services if necessary

The ICT manager – at Bowesfield this is OneIT

Commented [HL1]: Tanya/ Mickey or One itss?

The ICT manager is responsible for:

Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Conducting a full security check and monitoring the school's ICT systems on a weekly basis (the DSLs receive a daily notification from Smoothwall, the monitoring and filtering system).

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Ensuring that any online safety incidents are logged so that they can be dealt with appropriately in line with this policy

All staff and volunteers

All staff, including contractors, agency staff and volunteers are responsible for:

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

Ensuring they have read and understand the digital images policy (Appendix 4)

Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's anti-bullying policy

Parents / carers

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with families on the school website.

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Read and understand the digital images policy, providing permission for images of their child if they choose to do so

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - UK Safer Internet Centre

Hot topics - Childnet International

Parent factsheet - Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Pupils with Additional Needs

Staff are aware that some pupils may require additional 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.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's anti bullying policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know

how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, exploring the reasons it occurs, the forms it may take and what the consequences can be. This will be done through targeted lessons, assemblies and at any relevant points where school staff judge it to be useful to reinforce this learning with pupils.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Remote learning

In the event that children or staff need to provide or access school work remotely, school approved Learning Platforms and Virtual Learning Environments will be used.

Expectations of use will be in accordance with the schools acceptable use policies (Appendix 1-3) and staff social networking policy (appendix 6).

Commented [HL2]: Does any more than that need to be included as it is covered in the AUPs

Examining electronic devices

Pupils are not allowed to bring mobile phones to school. In the event that this does happen, school staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3. Acceptable Use Policies

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the computing lead or ICT manager (OneIT).

Work devices must be used solely for work activities.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL (and deputies) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection policy.

Use of personal mobile devices in school.

Staff and children must adhere to the mobile phone in school policy.

Misuse and monitoring

The DSL logs behaviour and safeguarding issues related to online safety.

Authorised staff may inspect any ICT equipment owned or leased by the School at any time without prior notice.

Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School 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.

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 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.

A breach or suspected breach of policy by a 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 School Disciplinary Procedures.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the DSL, computing lead or ICT manager. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID 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.

Review Procedure

There will be an on-going opportunity for staff to discuss with the DSL and computing lead any issue of online safety that concerns them.

This policy will be reviewed every 12 months by the Computing lead. At every review consideration given to the implications for future whole school development planning and will be shared with the governing body.

The policy will be amended as new technologies are adopted

This policy has been read and approved by the staff, head teacher and governors

Appendix 1 - Acceptable Use Policy: EYSF and KS1 pupils

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: Ask a teacher or adult if I can do so before using them Only use websites that a teacher or adult has told me or allowed me to use Tell my teacher immediately if: - I click on a website by mistake - I receive messages from people I don't know - I find anything that may upset or harm me or my friends - Use school computers for school work only I will be kind to others and not upset or be rude to them Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly Only use the username and password I have been given Try my hardest to remember my username and password Never share my password with anyone, including my friends. Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my parent/carer Save my work on the school network Check with my teacher before I print anything Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2 - Acceptable Use Policy: KS2 pupils

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** Always use the school's ICT systems and the internet responsibly and for educational purposes only Only use them when a teacher is present, or with a teacher's permission Keep my username and passwords safe and not share these with others Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my parent/carer Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others Always log off or shut down a computer when I'm finished working on it **I will not:** Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity Open any attachments in emails, or follow any links in emails, without first checking with a teacher Use any inappropriate language when communicating online, including in emails Log in to the school's network using someone else's details Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision Bring a mobile phone, tablet or other mobile device into school **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
1. **Parent/carer's agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3 - Staff ICT Acceptable Use Policy

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) Use them in any way which could harm the school's reputation Access social networking sites or chat rooms Use any improper language when communicating online, including in emails or other messaging services Install any unauthorised software, or connect unauthorised hardware or devices to the school's network Share my password with others or log in to the school's network using someone else's details Take photographs of pupils without checking with teachers first Share confidential information about the school, its pupils or staff, or other members of the community Access, modify or share data I'm not authorised to access, modify or share Promote private businesses, unless that business is directly related to the school

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I agree that the school may monitor the websites I visit and my use of the school's ICT facilities and systems to ensure AUP compliance. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team. I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4 - Digital Images Policy

Working with children and young people may involve the taking and recording of images – to record events in school or collect evidence of work for assessment.

Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people.

At Bowesfield, parents or carers are asked to sign to confirm that they are aware that images may be taken, and give their permission for this to happen, as their child is admitted to school. Children are informed of the reason for the photo being taken. The member of staff taking the photo needs to check photo permission prior to any photos being taken. Some parents / carers may agree to have their child's photo taken and used in displays in school, but not published anywhere other than in school, and not uploaded to the website. This must be discussed by individual staff with parents / carers and the discussion recorded on the permission booklet, initialled and dated by staff and parent / carer.

Information on the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the internet is included on the photo permission form.

All images must be taken only with school equipment and transferred within 1 school day to a file in staff shared / photographs, or deleted. As they are saved they must be deleted from the equipment. This is a secure area and only school staff have access to it. Photos will be saved until the children leave at the end of Y6 and then deleted.

Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings. If children appear uncomfortable for any reason, please allow them to choose not to be part of the photo.

It is not appropriate for adults to take photographs of children for their personal use.

All adults must ensure they:

- are clear about the purpose of the activity and about what will happen to the images when the activity is concluded
- are able to justify images of children in their possession and able to explain when they will transfer them to staff shared
- avoid making images in one to one situations or which show a single child with no surrounding context

Name of staff member/governor/volunteer/visitor:

signed (staff member/governor/volunteer or visitor):	**Date:**

Appendix 5 - Digital Images Policy: Parent Permission Slip

Photos of children are often used to record school events, or to use for assessment, and may be displayed and shared in the following ways. In the entrance of school, on the screen, for visitors and people in school to see On display boards around school On the school website On the websites of places that the children visit In the media, including online publications

We assure you that all staff have agreed to:

- Only take, and use photos as part of assessments, or when recording school events.
- Always consider the privacy, dignity, safety and well-being of your child.
- Only use school cameras, or other authorised equipment for photos of children.
- Promptly download images to a secure computer file, which only staff have access to.
- Immediately delete images from cameras.
- Permanently delete images from the file when your child leaves at the end of Y6.
- Not identify your child by name when displaying photos.

Any staff new to school will be asked to sign to say that they agree with this policy.

Visitors are asked not to have their mobiles / cameras in areas where there are children. If any other professionals ask to take photos as part of their work, they will have to follow the same guidance as school staff. For safeguarding reasons we need to have parental consent to take and use photos of children. Please sign the permission slip to give your consent for photos of your child to be taken and used, within the guidelines above, while they are at Bowesfield. If you have any concerns at all, at any time, please come and ask.

Name of child:	**Date:**
I give permission for photos of my child to be taken and used, within the guidance provided, while they attend Bowesfield Primary School. I understand that I have the right to change my mind and withdraw this permission at any time but that I must inform the school in writing of this.	
Signed (parent/carer):	**Date:**

Thank you for your support in keeping your child safe.

Appendix 6 - Staff Social Networking Policy

The Governing Body of Bowesfield Primary School is committed to ensuring that all staff are aware of their responsibilities in connection with the growing use of social networking sites. It recognises that the use of such sites have become a very significant part of life for many people. They provide a positive way to keep in touch with friends and colleagues, and can be used to exchange ideas and thoughts on common interests. Examples of such sites include, but are not limited to, blogs (short for web log), MySpace, Facebook, Bebo, YouTube, Windows Live Spaces, MSN, forums, bulletin boards, multiplayer online gaming, chatrooms and instant messenger.

Staff are expected to keep a professional distance from pupils and there should be a clear separation of the private social lives of staff and that of pupils. Any social networking with parents and children should be done using and approved social network page for the school in line with the acceptable use policy.

It is important that staff are able to use technologies and services effectively and flexibly whilst ensuring that they do not make themselves vulnerable. However, it is also important to ensure that this is balanced with the Governing Body's duty to safeguard children, the reputation of the school, the wider community and the Local Authority.

This policy will apply to all staff in schools whose contracts of employment have been issued by the Local Authority on behalf of the Governing Body, including Community and VA Schools. It does not apply to supply staff employed by agencies.

The policy aims to:

- Enable employees to use social networking sites safely and securely
- Ensure that employees are aware of the risks associated with the inappropriate use of social networking sites
- Safeguard employees in connection with the use of social networking sites and ensure they do not make themselves vulnerable
- Ensure the Governing Body maintains its duty to safeguard children, the reputation of the school, the wider community and the Local Authority

Legislation

The following legislation must be considered when adhering to this policy:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006

Responsibilities

The Governing Body (in conjunction with the Local Authority) shall:

- Ensure this policy is implemented and procedures are in place that deal with the use of social networking sites
- Ensure that all employees have access to this policy and that new employees are made aware of it

The Headteacher will:

- Be familiar with this policy and guidelines and ensure that employees understand the policy and their own responsibilities
- Ensure that staff are aware of the risks of the use of social networking sites and the possible implications of the inappropriate use of them
- Instigate disciplinary procedures where appropriate to do so
- Seek advice where necessary from Human Resources on the approach to be adopted if they are made aware of any potential issue.

Staff shall:

- Behave responsibly and professionally at all times in connection with the use of social networking sites;
- Co-operate with management in ensuring the implementation of this policy.

Human Resources shall:

- Provide the necessary professional advice and support to the Governing Body and all school staff when required.

Use of Social Networking Sites

For employees' own security all communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. It is therefore advised that staff follow the following procedures:

- Staff must not access social networking sites for personal use via school information systems or using school equipment;
- Staff must not accept pupils as friends – personal communication could be considered inappropriate and unprofessional and makes staff vulnerable to allegations;
- Staff are advised not to be friends with recent pupils.
- Staff should not place inappropriate photographs on any social network space;
- Staff should not post indecent remarks;
- If a member of staff receives messages on his/her social networking profile that they think could be from a pupil they must report it to their headteacher and discuss whether it is appropriate to contact the internet service or social networking provider so that they can investigate and take the appropriate action;
- Staff are advised not to write about their work but where a member of staff chooses to do so, he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the school/Local Authority. However, all other guidelines in this policy must be adhered to when making any reference to the workplace;
- Staff must not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act;
- Staff must not disclose any information about the school/Local Authority that is not yet in the public arena;
- In no circumstances should staff post photographs of pupils;

- Staff should not make defamatory remarks about the school/colleagues/pupils or the Local Authority or post anything that could potentially bring the school/Local Authority into disrepute;
- Staff should not disclose confidential information relating to his/her employment at the school;
- Care should be taken to avoid using language which could be deemed as offensive to others.

Breaches of the Policy

The Governing Body does not discourage staff from using social networking sites. However, all staff should be aware that the Governing Body will take seriously any occasions where the services are used inappropriately. If occasions arise of what could be deemed to be online bullying or harassment, these will be dealt with in the same way as other such instances.

If any instances of the inappropriate use of social networking sites are brought to the attention of the Headteacher, depending on the seriousness of the allegations, disciplinary action may be taken.

There may be instances where the School or Local Authority will be obliged to inform the police of any activity or behaviour for which there are concerns as to its legality.

Appendix 9 - Additional Guidance for Staff

e-Mail:

Managing e-Mail

The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to 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 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

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

The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder

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

E-mails created or received as part of your school job 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
- Inform a member of SLT if they receive an offensive e-mail

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

Sending e-Mails

If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information

- Use your own school 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
- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail
- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods

- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)
- Never open attachments from an untrusted source; Consult your network manager first.

When e-mailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using email - e-mailing confidential data is not recommended and should be avoided where possible

The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted

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

- Obtain express consent from your manager to provide the information by e-mail
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone) □
- Send the information as an encrypted document attached to an e-mail
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

Internet use

Managing the Internet

- Staff will preview any recommended sites before use
- Image searches are discouraged when working with pupils
- 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

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated

Infrastructure

- School internet access is controlled through the LA's gate keeper filtering service. For further information relating to filtering please go to a member of staff in school or contact the Stockton ICT Unit personally
- Our school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff are aware that internet activity can be monitored and explored further if required
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the DSL or ICT manager where appropriate.
- It is the responsibility of the school, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines
- Staff using removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems. All USB and removable devices must be encrypted.
- If there are any issues related to viruses or anti-virus software, the ICT manager should be informed

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to connect their ICT hardware to the school network points (unless provision has been made).
- 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's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- A time locking screensaver is applied to all machines. Any PCs etc. accessing personal data must have a locking screensaver as must any user profiles
- On termination of employment, resignation or transfer, return all ICT equipment. You must also provide details of all your system logons 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

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

Portable & Mobile ICT Equipment

- All activities carried out on School systems and hardware will be monitored
- Staff must ensure that all school data is stored on school's network, and not kept solely on a mobile device. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services
- 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
- Do not record passwords or encryption keys on paper or in an unprotected file
- Strong passwords are encouraged
- User ID and passwords for staff and pupils who have left the School are removed
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer).
- If you think your password may have been compromised or someone else has become aware of your password report this to the computing lead or ICT manager.

Computer Viruses

Never interfere with any anti-virus software installed on school ICT equipment that you use.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.