BEESTON HALL SCHOOL

7h - School E-Safety Policy 2021 - 2022

Introduction

The school community benefits from the opportunities provided by the internet and other technologies used in everyday life. However, there are associated risks and this policy outlines the measures taken to maximise the safety of the Beeston Hall School community. Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Agreements which all staff and children must follow.

As part of our commitment to E-safety, we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets. We have adopted the good practice requirements for all staff which are included in the staff handbook.

For the purposes of clarity and consistency throughout this document, the person in school who is taking a lead on E-safety is the Head of Department for IT. The Head of IT is responsible for this policy and will work with the Deputy Head and Designated Safeguarding Lead during the policy review.

Scope of the Policy

This policy applies to all members of Beeston Hall School (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of Beeston Hall School IT systems, both in and out of Beeston Hall School.

The Education and Inspections Act 2006 empowers the Headmaster to such extent as is reasonable to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying or other E-safety incidents covered by this policy which may take place outside of the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Beeston Hall School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate E- safety behaviour that takes place out of school.

Roles and Responsibilities

The following section outlines the E-safety roles and responsibilities of individuals and groups within Beeston Hall School.

Governors:

The responsibility of the Governors is to:

Read, understand, contribute to and help promote the school's E-safety policies and guidance as part of the school's overarching safeguarding procedures.

- Ensure appropriate funding and resources are available for the school to implement their E- safety strategy.

Governors are responsible for reviewing the effectiveness of the policy. This will be carried out by the Governor receiving regular information about E-safety incidents and monitoring reports (Governor responsible for safeguarding).

This role includes:

- Regular meetings with the Designated Safeguarding Lead
- Regular monitoring of E-safety incident logs
- Regular monitoring of filtering control logs
- Reporting to relevant Governors

Headmaster:

- The Headmaster has a duty of care for ensuring the safety (including E-safety) of members of the school community, though the day-to-day responsibility for E-safety will be delegated to the Head of IT.
- The Headmaster and Designated Safeguarding Lead are aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff (see flow chart on dealing with E-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR/other relevant body disciplinary procedures).
- The Headmaster is responsible for ensuring that the Head of IT and Designated Safeguarding Lead receive suitable training to enable them to carry out their E-safety roles and to train other colleagues, as relevant.
- The Headmaster will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role.
- The Senior Leadership Team will receive regular monitoring reports from the person nominated to monitor internal E-safety reports.
- The Head of IT monitors the annual E-safety Policy review.

Head of IT:

- Leads on E-safety issues.
- Takes day-to-day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school technical staff.
  Receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments.
- Meets regularly with DSL to discuss current issues, review incident logs and filtering/change control logs.
- Reports to the Senior Management Team as necessary.
- Ensures that the school meets required E-safety national policy guidance.
- Ensures that users may only access the networks and devices through a properly enforced password protection policy in which passwords are regularly changed.
- Ensures that they keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant.

Premier Links (External IT Support) - Tim Cole (Internal IT Support).

- Ensures that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensures that monitoring software/systems are implemented and updated as agreed in school policies.
- Ensures that the use of the network, Internet, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Deputy Head or Headmaster for investigationTeaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of E-safety matters and of the current school E-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement (Appendix 2) and Bring Your Own Device (BYOD) policy (Appendix 3).
- They report any suspected misuse or problem to the Head of IT and relevant form tutor for investigation/action/sanction.
- All digital communications with children/parents/carers should be on a professional level and only carried out using official school systems.

- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Children understand and follow the E-safety and acceptable use agreements.
- Children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where Internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches

Designated Safeguarding Lead (DSL):

The Designated Safeguarding Lead is trained in E-safety issues and is aware of the potential for serious child protection/safeguarding issues that arises from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying

The DSL will also:

- Liaise with the Local Authority/relevant body
- Meet with the Head of IT to discuss current issues, review incident logs and filtering/change control logs.
- Meet with the Safeguarding governor to discuss current issues, review incident logs and filtering/change control logs.

Children:

- Are responsible for using the school digital technology systems in accordance with the Acceptable Use Agreement for children (Appendix 4).
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyberbullying.
- Should understand the importance of adopting good E-safety practice when using digital

technologies out of school and realise that the school's E-safety Policy covers their actions out of school if related to their membership of the school.

Parents/Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, and information about national/local E-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website/VLE and online student records.
- The personal devices belonging to their children.

The school safeguarding leaflet for visitors contains guidance for the use of cameras at school events.

Policy Statements

Education – children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

Safety is a focus in all areas of the curriculum and staff should reinforce E-safety messages across the curriculum. The E-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned E-safety curriculum is provided as part of Computing/PHSE/other lessons and is being regularly revisited. Every pupil in the school completes a course of E-safety lessons as part of their IT Programme of Study.

- Key E-safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities. In tutor groups and as part of PSHEE, E-safety is covered as part of our pastoral care.
- Children are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information. Children are taught in IT lessons how to use emails and the internet correctly and safely.
- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Children are helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school at the start of each School Year. The pupils cover and agree to an Acceptable Use Agreement. This covers the standard of behaviour and use that is expected of the children when using the Beeston Hall Network. A copy may be found on the School Website. This is also reinforced throughout the teaching year.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- The School arranges visits from external professionals to speak to the pupils about safety in the digital world.
- In lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where children can freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, children may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Head of IT can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Technical – infrastructure/equipment, filtering and monitoring:

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements. Instead of relying on one system, the school has five layers of protection in place.
- The first of these is 'Draytek fire wall', a piece of hardware connected to the Server which controls incoming and outgoing Internet/email traffic, blocking at source unsuitable websites/emails. F secure is layered on top of this to deal with more filtering and protection. Impero Management Systems utilises remote access control to block and filter real-time web traffic and monitor the use of the Internet. Google Safe Search and Google Management Console filters web content on web browsers. Active Directory on our Windows Server System helps control and filter user access. Lastly, and very importantly, staff make regularly checks during break times.

- There are reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school systems and devices.
- All users will be provided with a username and secure password. Users are responsible for

the security of their username and password.

- The school has provided enhanced/differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) to the school systems.
- An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.
- Users are not permitted to download and/or install applications (including executable or similar types) on to a school device or whilst using the school's systems without agreement from the Head of Computing.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act).
- To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other children in the digital/video images.
- Staff and volunteers can take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal

equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website.
- Children's work can only be published with the permission of the child's and parents or carers.

Data Protection

The school recognises its obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We annually review our practices and procedures to ensure that they meet this basic obligation.

Pupils are taught about the need to protect their own personal data as part of their E-safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data, including the following:

- Staff are provided with appropriate levels of access to the school's management information systems holding pupil data. Passwords are not shared, and administrator passwords are kept securely.
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school.
- When we dispose of old computers and other equipment, we take due regard for destroying information which may be held on them.
- Remote access to computers is by authorised personnel only.
- We have full back-up and recovery procedures in place for school data.

Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example Governors or the Senior Designated Child Protection Officer, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any

spare copies. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the school's Data Protection Policy.

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data. Classroom computers must always be logged off when a member of staff leaves a room unattended.
- Transfer data using encryption and secure password-protected devices.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Users should be aware that email communications are monitored at the Headmaster's discretion.
- Users must immediately report to the Designated Safeguarding Lead, the Deputy Head or the Headmaster the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and children or parents/carers must be professional in tone and content.
- Children should be taught about E-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school/ website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for children and staff. Schools and local authorities could indirectly be held responsible for acts of their employees during their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school

or local authority liable to the injured party. Reasonable steps to prevent predictable harm are in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children, staff and the school through limiting access to personal information:

- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.
- School staff should ensure that:
- No reference should be made in social media to children, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Headmaster. Pupils are taught about the need to protect their own personal data as part of their E- safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures and, where necessary, training, are in place to ensure the security of such data including the following:

- Staff are provided with appropriate levels of access to the school's management information systems holding pupil data. Passwords are not shared, and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school.
- When we dispose of old computers and other equipment, we take due regard for destroying information which may be held on them
- Remote access to computers is by authorised personnel only.
- We have full back-up and recovery procedures in place for school data.

Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example Governors or the Designated Safeguarding Lead, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies

PERSONAL USE OF SOCIAL MEDIA

We recognise that staff may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the organisation's business are also prohibited. Staff must ensure that their use of social media does not create any breaches of Internet security and therefore must be careful to avoid any applications that might interrupt our IT systems. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.

We prohibit staff from using their work email address for any personal use of social media.

THE MONITORING OF SOCIAL MEDIA

The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including, but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

We may store copies of such data or communications for a period after they are created and may delete such copies from time to time without notice.

Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

SOCIAL MEDIA AND THE END OF EMPLOYMENT

If a member of staff's employment with our school should end, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that you are no longer employed or associated with our school

All professional contacts that a member of staff have made through their course of employment with us belong to our school, regardless of whether the member of staff has made social media connections with them.

Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the network so that they can obtain age-appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered Internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should be aware of the E-safety Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school, keep under file with a signed copy returned to the member of staff.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the Internet or learning platform in an abusive or illegal manner, a report must be made to the Headmaster immediately and then the Whistleblowing Policy and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an email to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

Beeston Hall School will encourage parents/carers to support with their child or young person. This can be shown by viewing the Acceptable Use Agreements on the website together so that it is clear to the school/education setting or other establishment that the agreement is accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond school.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate. The downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose' based on research for work and be copyright-free.

File-sharing via email, weblogs or any other means online should be appropriate and be copyright-free when using the learning platform in or beyond school.

The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal):

- accessing inappropriate or illegal content deliberately.
- deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- continuing to send or post material regarded as harassment or of a bullying nature after being warned (see the Cyber Bullying Policy in Appendix 1).
- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites).

The following activities are likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message or create content that is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act, revised 1988

The following activities would normally be unacceptable; however, in some circumstances they may be allowed e.g. as part of planned curriculum activity or as system administrator to problem- solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time.
- sharing a username and password with others or allowing another person to log in using your account.
- accessing school IT systems with someone else's username and password.
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else.

In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any child found to be misusing the Internet by not following the Acceptable Use Agreement may incur a sanction relevant to the breach of the Acceptable Use Agreement.
- Further misuse of the agreement may result in further sanctions in accordance with the **Rewards and Sanctions policy**.
- If the matter is a safeguarding issue, then the school's **Safeguarding Policy** will be followed.

If a child or young person **accidentally** accesses inappropriate materials, the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications of misusing the Internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Responding to incidents of misuse:

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "In the Event of Inappropriate Use" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images or if there is any other suspected illegal activity, see the procedure set out below for responding to online safety incidents and report immediately to the police.

The Deputy Head investigates inappropriate staff use.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

1. The Deputy Head, Head of IT and the child's Form Tutor will investigate the issue.
2. Conduct the procedure using a designated computer that will not be used by young

people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

3. It is important to ensure that the relevant staff should have appropriate Internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
4. Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
5. Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action.
    - If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:
        - Incidents of 'grooming' behaviour.
        - The sending of obscene materials to a child.
        - Adult material which potentially breaches the Obscene Publications Act.
        - Criminally racist material.
        - Other criminal conduct, activity or materials.
    - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Reviewed by: Bob Hammond, Adam Davies and Paul Leaver September 2021

Next scheduled review: September 2020

Appendix 1

BEESTON HALL SCHOOL

Cyberbullying Policy

Safeguarding and Computing

Protecting young people in the online world means thinking beyond the school environment. As well as the computer to access the Internet, now many mobile phones and games consoles offer broadband connections.

Increasingly pupils will have access to personal devices not covered by network protection and therefore the emphasis needs to be on educating all users as to the risks involved and their obligation to act responsibly while online.

Safeguarding pupils in both the real and virtual world is everyone's responsibility and all staff at Beeston Hall School should be aware of this policy and how to respond to E-safety incidents.

Should be replaced with: The pupils receive a course of six E-safety lessons at the start of each school year and this partly covers aspects of cyber-bullying.

In addition, pupils receive a lesson twice a year covering the Acceptable Use of the Beeston Hall Network. In parts, this also refers to their responsibilities in using the Internet and emails.

All pupils are made aware of the Acceptable Use Agreement and what to do if they have any computing safeguarding concerns.

Procedures for dealing with Inappropriate/Illegal Internet Access or Material

If staff or pupils discover unsuitable websites, this should be immediately reported to the Head of Pastoral Care who, in liaison with the Headmaster and Head of Computing will consider a referral to the Internet Watch Foundation (IWF) and the Police.

What to do in the event of discovery of illegal material:

- Seek immediate and specific advice from the Deputy Head Pastoral who will consult with the Head of Computing and the Headmaster. They may contact the Police or social services, dependent on the severity of the case.
- The Head of Computing will prevent any further access to the material.
- Evidence should be collected from back-up-software, Filter and Monitoring Applications.
- Under no circumstances should the Headmaster, Deputy Head Pastoral or Head of Computing attempt to investigate on their own or bring in an outside expert to do so as this may compromise the evidence if a legal case were to result.

In some cases, this may constitute a criminal offence.

Combating Cyberbullying

Cyberbullying can be defined as 'the use of Information and Communications Technology (ICT), particularly mobile phones and the Internet, deliberately to upset someone else'. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target.

However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages, the size of the audience, perceived anonymity, even the profile of the person doing the bullying and their target.

Cyberbullying takes different forms: threats and intimidation, harassment or 'cyberstalking' (e.g. repeatedly sending unwanted texts or instant messages), vilification/defamation; exclusion or peer rejection, impersonation, unauthorised publication of private information or images and manipulation.

Some cyberbullying is clearly deliberate and aggressive, but it is important to recognise that some incidents of cyberbullying are known to be unintentional and the result of simply not thinking about the consequences.

What may be sent as a joke may not be received as one, and indeed the distance that technology allows in communication means the sender may not see the impact of the message on the receiver. In cyberbullying, bystanders can easily become perpetrators, e.g. by passing on or showing to others, images designed to humiliate, or by taking part in online polls or discussion groups.

They may not recognise themselves as participating in bullying, but their involvement compounds the misery for the person targeted.

'Bystanders' – better termed 'accessories' in this context – who actively support cyberbullying are attributed to the case and the school's Anti- Bullying Policy will apply.

It is important that pupils are aware that their actions have severe and distressing consequences, and that participating in such activity will not be tolerated. There are features of cyberbullying that differ from other forms of bullying which need to be recognised and considered when determining how to respond effectively.

The key differences are:

Impact — the scale and scope of cyberbullying can be greater than other forms of bullying.

Targets and perpetrators — the people involved may have a different profile to traditional bullies and their targets.

Location — the 24/7 and any-place nature of cyberbullying.

Anonymity — the person being bullied will not always know who is attacking them.

Motivation — some pupils may not be aware that what they are doing is bullying.

Evidence — unlike other forms of bullying, the target of the bullying will have evidence of its occurrence.

Prevention

We seek to instill values in all members of Beeston Hall School, which should, ideally, preclude all bullying. These are reinforced in our PSHE programme and IT lessons covering E-safety.

These seek to instill respect for others, their property and their individuality. We hope these values underpin ordinary curricular lessons too.

It is crucial to the school's success in dealing with cyberbullying that all members of the community are made aware that it is unacceptable and should not be tolerated. It is the responsibility of all members of the community to act if they are aware of it happening. To remain silent is to condone the action of the bully. On the school website is information for parents and carers about cyberbullying and how they can help.

Process

Information is crucial to dealing with the problem. Those who feel that they are being bullied, or who are witnesses to what they believe is bullying/cyberbullying, should always tell a member of staff.

Advice, support and counselling will be offered to all parties involved, and, if necessary, their parents.

While recognising that both victim and bully need help, we do not adopt a 'no blame' position.

If a pupil receives an abusive e-mail or text, they should report the matter to a member of staff as soon as possible.

The case will be taken up by the relevant Form Tutor.

The victim's Form Tutor and where necessary the Deputy Head will see the victim and (unless the case is very serious) any witnesses without delay and form an initial view of the allegation:

- Is the child suffering or likely to suffer significant harm? If so, the DSL will be informed, and the safeguarding procedure will take place.
- The nature of the incident/s – physical? verbal? exclusionary? Etc.
- Is it a "one-off" incident involving an individual or a group?
- Is it part of a pattern of behaviour by an individual or a group?
- Has physical injury been caused? Who should be informed – the Headmaster? Parents? The school's Designated Safeguarding Lead? Social Services? The police?
- Can the alleged bully be seen on a no-names basis?
- What is the likely outcome if the complaint proves to be correct?

Sanctions

In practice, the sanctions applied range from a verbal warning or a ban on use of the school's computer network to a temporary or permanent exclusion, depending on the gravity of the

offence and the pupil's previous record with reference to bullying/cyberbullying.

The aim of sanctions is to:

- Help the person harmed to feel safe again and be assured that the bullying will stop.
- Hold the perpetrator to account, getting them to recognise the harm caused and deter them from repeating the behaviour.

- Demonstrate to the school community that cyberbullying is unacceptable and that the school has effective ways of dealing with it, thus deterring others from behaving similarly.

When cyberbullying is investigated, reference will be made to the Acceptable Use Agreement.

Technology-specific sanctions for pupils engaged in cyberbullying behaviour could include limiting Internet access for a period or removing the right to bring a mobile phone into school (although issues of child safety will be considered in relation to the latter).

Cyberbullying will have an impact on the education and wellbeing of the person being bullied, and the physical location of the bully at the time of their action is irrelevant in this.

Schools now have broad new powers to discipline and regulate the behaviour of pupils, even when they are off the school site. These are set out in the Education and Inspections Act 2006. Misconduct of any kind outside of school will be amenable to school discipline if the welfare of another pupil or the culture or reputation of the school is placed at risk.

Staff

There is also a possibility that the Staff at Beeston Hall School could be cyberbullied. If any member of Staff feels they are being cyberbullied, they shouldlet either of the Deputy Head's know immediately. If the perpetrator is one of the Deputy Head;s, the Headmaster should be informed.

Anti-Cyberbullying Code: Advice to pupils

Advice is giving to Pupils in E-safety lessons, by tutors, in PSHEE and occasionally by lectures and visitors. This is wide in range and may include videos, discussion, talks and activities.

Being sent an abusive or threatening text message or seeing nasty comments about yourself on a website can be really upsetting.

This code gives you five important tips to protect yourself and your friends from getting caught up in cyberbullying, and advice on to how to report it if it does happen.

1. **SAFE**

   Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number

and password.

2. **MEETING**

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then, only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

3. **ACCEPTING**

Accepting emails, instant messages, or opening files, pictures or texts from people you don't know, or trust can lead to problems – they may contain viruses or nasty messages.

4. **RELIABLE**

Someone online might lie about who they are and information on the Internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online, it's best to only chat to your real-world friends and family.

5. **TELL**

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

Reviewed: September **2021**

Next review date: Sept 2022

APPENDIX 2

BRING YOUR OWN DEVICE (BYOD) AGREEMENT FOR STAFF AND VISITORS

The school recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective and to visitors. Our school embraces this technology but requires that it is used in an acceptable and responsible way. This policy is intended to address the use by staff members and visitors to the school of non-school owned electronic devices. For the purposes of this policy the term 'visitors' includes parents, nominated carers and guardians.

School staff should read this policy alongside the *Acceptable Use of Personal Mobile Devices Agreement*.

General Guidelines

All school staff must observe the following guidelines:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access;
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school;
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home);
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues;
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs must be set on personal devices to aid security;
- The school is not responsible for the day to day maintenance or upkeep of the staff personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues;
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances;
- Printing from personal devices will not be possible.

Compliance with the General Data Protection Regulation

Staff compliance with this BYOD policy is an important part of the school's compliance with the *General Data Protection Regulation* (GDPR May 2018). Staff must therefore apply this BYOD policy consistently with the school's *Data Protection Policy.*

It must be acknowledged that BYOD raises several data protection concerns because the device is owned by the user rather than the data controller. The school, as data controller, will ensure that all processing for personal data remains in compliance with the GDPR. Particularly in the event of a security breach, the data controller will be able to demonstrate that they have secured, controlled or deleted all personal data on a device.

Staff must adhere to the following good practice to ensure the risk of data breach is minimised:

- Use a strong password to secure your device;
- Use encryption to store data on the device securely;
- Ensure that access to the device is locked or data automatically deleted if an incorrect password is input too many times;
- Ensure that the device automatically locks if inactive for a period;
- Maintain a clear separation between the personal data processed on behalf of the data controller and that processed for the device owner's own purposes, for example, by using different apps for school and personal use.

Support

The school takes no responsibility for supporting staff's own devices; nor has the school a responsibility for conducting annual PAT testing of personally-owned devices.

Compliance, Sanctions and Disciplinary Matters for staff

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs the school will respond according to the disciplinary procedures outlined in the Staff Handbook. Guidance will also be offered.

Incidents and Response

The school takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the mobile device should be reported to the Bursar. Data breaches and other data protection incidents must be reported to, and recorded by, the Bursar as soon as practicably possible.

Use of Cameras and Filming Equipment (including mobile phones) by Parents and Guardians

Parents, guardians or close family members (hereafter, parents) are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the School expects all parents to follow:

- When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; The School therefore asks that it is not used at indoor events.
- Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.
- Parents are reminded that such images are for personal use only. Images which may, expressly or not, identify other pupils should not be made accessible to others via the internet (for example on Facebook or YouTube), or published in any other way.
- Parents are reminded that copyright issues may prevent the School from permitting the filming or recording of some plays and concerts. The School will always print a reminder in the programme of events where issues of copyright apply.
- Parents may not film or take photographs in changing rooms or backstage during school productions, nor in any other circumstances in which photography or filming may potentially embarrass or upset pupils.
- The School reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.
- The School sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case CD, DVD or digital copies may be made available to parents for purchase. Parents of pupils taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.
- Parents reserve the right to opt out of their child/children (a) being photographed or (b) identifiable images of their child being used in publicity material.
- The School may, at any event, refuse to allow the taking of photographs or film. Though comprehensive, this policy cannot be guaranteed to cover every eventuality. Under all circumstances, however, the safeguarding of the children in the school's care is paramount.

Reviewed: September 2021
Next review: September 2022

BEESTON HALL SCHOOL

Appendix 3

ACCEPTABLE USE OF PERSONAL MOBILE DEVICES AGREEMENT

We as a school accept and are grateful for the staff provision (should they wish) of their own mobile devices in assisting with the efficient operation of the school. However, all staff must accept that the safeguarding of both pupils and staff takes priority when personal mobile devices are used.

When reading and signing this agreement staff understand that the primary purpose of having their personal mobile device at school is educational and that this is irrespective of whether the device is school-owned/-provided or personally owned.

This Acceptable Use Agreement sits alongside a range of polices including, but not limited to, the Safeguarding Policy, the IT Policy, the Bring Your Own Device Agreement, policies around theft or malicious damage and the Pastoral Care Policy. Please also be aware that teaching about the safe and appropriate use of mobile technologies is included in the online safety education programme as part of the school's provision for PSHEE and Computing.

For completion by all staff:

I understand and accept the following points which govern the use of personal mobile and internet-enabled devices (to include phones, tablets, cameras and other similar electronic devices) at school or in connection with school life.

I accept mobile devices are useful additions to the education and safe management of children in Beeston Hall's care should I wish to use them, but with the proviso of utmost caution, for the safeguarding of myself as well as children in my care. I agree with and accept that:

- Mobile devices are never to be taken into the Pre-Prep area (under EYFS guidelines) or any area where Pre-Prep children may be present.
- Mobile devices are never to be taken into the changing rooms.
- Mobile devices are to be kept out of sight - in either a pocket or a bag, a locked cupboard or staff pigeonholes when not in use for school-related reasons.
- Staff-owned mobile phone devices should not be used for personal purposes during teaching sessions.
- Mobile phone devices must be in silent mode on the school site.
- Mobile devices are not to be taken into the boarders' accommodation.
- Mobile phones may only be answered in areas where there are no children present i.e.

Common Room, staff workroom, maintenance area or office.

- Any photograph taken of a child/children using a personal mobile device during school duties will be deleted as soon as possible and certainly within 24 hours and children will be notified first of purpose and intention. For the sake of clarity staff must only take pictures or videos that are required for an educational task or activity or school news reporting and marketing. All unnecessary images or videos will be deleted immediately.
- passcode (e.g. pin number or password) should be set and used on the device. Whenever possible, use a strong passcode which must not be shared with anyone. The device must be set to lock automatically when it is inactive for more than a few minutes. (Similarly, staff must always log out of a classroom computer when leaving the room; further detail on that is contained in the Staff Handbook and IT Policy).

I understand that if I fail to comply with these requirements, this may constitute a breach of the Code of Conduct and become a matter subject to disciplinary action.

Signature: ..... Date: .....

Print Name: ..... Role: .....

APPENDIX 4 ACCEPTABLE USE POLICY – CHILDREN

The computers on the school network are provided and maintained for the benefit of all pupils, and you are encouraged to use and enjoy these resources and help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the internet. General:

- The use of the computers is not a right but a privilege that may be removed at any time.
- **The use of the internet is monitored and recorded accordingly.**
- Your email account may be monitored and removed if not used properly.
- **You are responsible for observing the advice on E-safety that is given to you in lessons.**

Computer Room and Devices

- You are expected to behave in the Computer Room and use the devices with care.
- **You must not use any hardware (except the computers) in the Computer Room without permission of staff.**
- Do not attempt to attach your own device or try to open the computers.
- **Do not use any flash drives or removable media without permission from a member of staff.**

The Internet

- Only access suitable material. Unpleasant, unlawful, obscene or abusive material is not permitted.
- **You must report any unpleasant or suspicious material to a member of staff.**
- You must not download games or use social media web sites (e.g. Facebook, Instagram) at school.
- **You are not allowed to buy and sell items on the internet whilst you are at school.**
- You must not undertake any online activity which is likely to adversely impact on the reputation of the school.

Email

- You may only use the email account provided to you by the school.
- **You must be polite and not send bullying, rude or threatening emails to anyone.**
- Immediately report any unpleasant emails that you receive to a member of staff.
- **Only open attachments to emails if they come from someone you already know and trust.**

Security

- You must not use someone else's username/password to gain access to the school network.
- **Any internet connected devices brought into school must be given into tutors/matrons.**
- You may only use internet connected devices on school trips with the permission of staff.
- **Do not give any details about yourself when you are online**

Reviewed: September 2021

Next review: September 2022*