E-SAFETY POLICY

June 2020

Policy Consultation & Review

This policy is available on our school website and is available on request from the school office. We also inform parents and carers about this policy when their children are referred to the Beacon of Light School.

The policy is provided to all staff (including temporary staff and volunteers) at induction.

This policy should be read in conjunction with school Behaviour Policy and Safeguarding Policy. This policy should be read alongside the Addendum to the Child Protection Policy, Addendum to the Teaching and Learning Policy, Addendum to the Safeguarding Policy and the Remote Learning Policy.

This policy will be reviewed in full by the Trustees on a bi-annual basis. This policy was last reviewed and agreed by the Trustees in June 2020.

Signature Principal Date:

Signature Chair of Trustees Date:

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Trustees: May 2020. Monitoring of the E-Safety Policy will take place at regular intervals. The Trustees will receive a report on the implementation of the E-Safety Policy on a half termly basis. Please see Appendix 1 for an example of the report presented to Trustees.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be May 2021.

This E-Safety policy should be read in relation with the Beacon od Lights following policies:

- Child Protection Policy
- Teaching and Learning Policy
- Remote Learning Policy

This policy also covers the use of ICT in the event of a school closure (Appendix 8)

The school will monitor the impact of the policy using:

- Logs of reported incidents sent weekly to the delegated member of staff responsible for E-Safety by the Foundation of Light ICT Support
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of:
  - students
  - parents/carers
  - staff

Definition of E-Safety

The term 'safeguarding' is defined for the purposes of this document in relation to Online Safety as the process of limiting risks to children when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection.

The Beacon of Light School has adopted the definition of Online Safety (or e-Safety) as the safeguarding of children and young people in the digital and online world. Therefore, this encompasses not only internet technologies but also mobile phones, gaming consoles plus other devices and technologies. Online safety must be to be considered as part of all professionals' wider safeguarding responsibilities.

It must be recognised that online safety is not a technological issue and should not just be limited to settings where children have access to technology.

Responsibility for online safety should not be delegated to colleagues with technical responsibilities or ICT/computing teaching, but must be firmly embedded within safeguarding policies, practices and responsibilities. Safeguarding is the responsibility of all staff in all settings and agencies.

Online Safety is about educating children and young people about the benefits and responsibilities of using information technology safely. Restricting access to technology plays a limited role. In this document, as in the Children Act 1989 and the Children Act 2004, a child is defined as anyone who has not yet reached their eighteenth birthday. Where we use the word 'child' (or its derivatives) in this document, we mean 'child or young person'.

Terms such as 'e-Safety', 'online', 'communication technologies' and 'digital technologies', when used in this document, refer to all fixed and mobile technologies that children may encounter, now and in the future, which allow them access to content and communications that could raise online safety issues or pose risks to their well-being and safety.

As in any other area of life, children and young people can be vulnerable and may expose themselves to dangers: either knowingly or unknowingly when using the internet and other digital technologies. Particular concerns may affect children and young people considered to be more vulnerable if they have special educational needs as such children may not understand concepts such as “safe” unless in a specific situation.

Online safety is not just about safeguarding children and young people, it is also important to ensure that professionals and parents/carers are educated to enable them to prepare children for the digital world. Professionals also need clear advice and boundaries regarding safe online practice in order to protect themselves and the reputation of their organisations.

Online safety concerns may include:

- Exposure to inappropriate or harmful material online e.g. gambling content, pornography or violent content
- Bullying via technology (known as online or cyberbullying)
- Exposure to illegal material such as indecent images of children
- Children and young people creating and sharing youth produced sexual images of themselves or their peers (known as sexting
- “Digital” self-harm
- The threat of danger from contacting unsuitable adults or peers via social networking sites, gaming, instant messaging or chat rooms
- Use of technology within child sexual exploitation
- Problematic internet use (internet “addiction”)
- Exposure to content that promotes worrying or harmful behaviour e.g. suicide, self-harm and eating disorders
- Becoming victims of cybercrime such as hacking, scams/hoaxes, fraud and identity theft
- Becoming a perpetrator of cybercrime such as hacking and piracy
- Radicalisation and extremism online
- Publishing too much personal information online

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students 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 cyber- bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is 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.

Beacon of Light 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 take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Beacon of Light School.

Trustees:

Trustees are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about e-safety incidents and monitoring reports. A member of the Trustees has taken on the role of E-Safety Trustee. The role of the E-Safety Trustee / Director will include:

- regular meetings with the E-Safety Coordinator (Principal, or the member of staff to which that role has been delegated)
- regular monitoring of e-safety incident logs through the challenge of the report on a half termly basis
- regular monitoring of filtering/change control logs

Principal and Senior Leaders:

- The Principal 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 E-Safety Coordinator (Principal).

- The Principal and (at least) another member of the Senior Leadership Team should be 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 Principal/Senior Leadership Team are responsible for ensuring that the E-Safety Coordinator (Curriculum Lead for ICT) receives suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Principal and the delegated member of staff responsible for E-Safety 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The delegated member of staff responsible for E-Safety will receive weekly reports from the Foundation of Light ICT report. Any concerns found within the report will be reported, using the E-Safety report log, to the SLT.

- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Coordinator/ Designated Senior Person.

- Liaise with Curriculum Lead for ICT on E Safety Logs and implementing updated E-Safety procedures. This will be done half termly to discuss the Trustees Report, or as required due to concerns raised.

E-Safety Coordinator (Principal and the member of staff which has been delegated the responsibility for E-Safety):

- 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 the Local Authority/relevant body
- Liaises with school technical staff and Curriculum Lead for ICT who has been delegated the responsibly for E-Safety by the Principal.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e- safety developments
- Meets regularly with E-Safety Trustee to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meeting/committee of Trustees
- Reports regularly to Senior Leadership Team
- Review reports received from the Foundation of Light ICT Support on a weekly basis and reports any concerns to the SLT (Please see Appendix 7)
- Ensure the Statutory guidance from the DfE on the Teaching of E-safety is adhered to across school and that all areas of the guidance are delivered to the students.

IT Network Manager:

The IT Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

- 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.

- That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal/ E-Safety Coordinator (Curriculum Lead for ICT) for investigation/action/sanction. Reports on ICT usage must be produced weekly and shared with the Curriculum Lead for ICT

- That monitoring software/systems are implemented and updated as agreed in school policies.

- Produces weekly reports on network safety logs and presented to E-Safety coordinator or the designated person.

- Report any E-Safety issues immediately to the E-Safety coordinator.

Teaching 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.

- They report any suspected misuse or problem to the Principal/E-Safety Coordinator (Curriculum Lead for ICT) for investigation/action/sanction. Use Appendix 7 to refer concerns to the E-Safety coordinator.

- All digital communications with students/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.

- Students understand and follow the e-safety and acceptable use agreements.

- Students 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 students 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

- The member of staff leading the session is responsible for the monitoring the use of ICT within the classroom, including the use of staff laptops and blocked websites. They must report any breaches to the code of contact to the E-Safety Coordinator immediately and follow this up with the written referral within Appendix 7.

- Students must not be allowed to use staff laptops, when logged into a staff account due to the different level of restrictions placed on staff and students accounts. Should a student access a staff laptop during a lesson this must be reported immediately to the E-Safety Co-coordinator, then followed up with the written referral within Appendix 7.

Child Protection/Safeguarding Designated Person (Principal):

The Child Protection/Safeguarding Designated Person should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data

- Access to illegal/inappropriate materials

- Inappropriate on-line contact with adults/strangers

- Potential or actual incidents of grooming

- Cyber-bullying

- Sexting

- County Lines

Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement.

- 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 cyber-bullying.

- 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, letters, website/VLE 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 on-line student records.
- Their children's personal devices in the school (where this is allowed)

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach in line with the DfE Guidance issued in September 2019. The education of students 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.

E-safety should be 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 should be provided as part of ICT/PHSE/other lessons and should be regularly revisited.

- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- In lessons where internet use is pre-planned, it is best practice that students 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. It is the responsibility of the member of staff leading the session to monitor the use of ICT within the classroom, they must report any breaches to the E-Safety Coordinator immediately and follow this up with a written referral within Appendix 7.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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. This will need to be done at least one week prior to the lesson during which the topic is being taught to allow the E-safety Coordinator time to arrange this with the Foundation of Light ICT Support.

• Students will take part in wider events linked to E-Safety such as E-Safety Day.

• Student will sign a ICT Acceptable Usage Agreement as part of the induction meeting

Education – parents/carers:

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

Education – The Wider Community:

The school will provide opportunities for local community groups/members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- The school website will provide e-safety information for the wider community

Education & Training – Staff/Volunteers:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned program of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. This will be coordinated by the E-Safety Coordinator.

- All new staff should receive e-safety training as part of their induction program, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.

- The E-Safety Coordinator (Curriculum Lead for ICT) will receive regular updates through attendance at external training events/other relevant organisations and by reviewing guidance documents released by relevant organisations.

- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.

- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

- Sign the acceptable usage statement, please refer to Appendix 2, and return this to the E-Safety Coordinator.

Training – Trustees:

Trustees should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Trustees Association/or other relevant organisation.

- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring:

The school will be 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

- There will be regular reviews and audits of the safety and security of school technical systems. This will be monitored on a weekly basis and reports will be shared with the E-Safety

Coordinator.

- 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. These will either be identified from the weekly reports provided to the E-Safety Coordinator or reported by staff immediately to the E-Safety Coordinator and followed up with the referral form within Appendix 7.

- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto 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 IT department.

- Users must not use personal devices to teach or store images of students on

- Users may use the following types of removable media for the purposes detailed:

    - CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
    - USB Media (memory sticks) – this type of media can be used on school devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
    - Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

Bring Your Own Device (BYOD):

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

We do not encourage students bringing their own devices into school and request that all mobile phones are handed in on arrival.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Students receive training and guidance on the use of personal devices.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss, theft, change of ownership of the device will be reported.

Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students 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 students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, 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 students in the digital/video images.

- Staff and volunteers are allowed to 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Students must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers around the use of a student's image is gained within the induction meeting.

- Student's work can only be published with the permission of the student and parents or carers.

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data

Protection Act 1998 and the schools' Data Protection Policy. Staff must ensure that they:

- At all times take care to ensure the safe keeping 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.

- Transfer data using encryption and secure password protected devices.

  Please see Appendix 2

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 and is monitored. Users should be aware that email communications are monitored. All electronic communications with parents and students should be through the designated school email.

- Users must immediately report, to the nominated person – in accordance with the school policy, 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 students or parents/carers (email, chat, VLE etc.) must be professional in tone and content.

- Students 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.

- The Beacon of Light School has decided not to complete Online Counselling following advice from Safeguarding First but will conduct a student voice activity covering their social and emotional health. This was introduced and is conducted weekly from 6th March. WG then monitors responses and signposts the family to appropriate support on an individual basis. The Beacon of Light School works with Kooth. This is an online mental health provider for children. All staff have received training from Kooth representatives.

Social Media - Protecting Professional Identity:

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of 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 must be in place.

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

- Training to include acceptable use; social media risks; checking of settings; data protection; reporting issues.

- Clear reporting guidance, including responsibilities, procedures and sanctions.

- Risk assessment, including legal risk.

- If a member of staff is contacted by a student on Social Media. They screenshot the contact and email it to the SLT. In the presence of a member of the SLT, they then block the student from making further contact.

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff or refer to the current COVID-19 school closures.

- 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. 11

- 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 and is coordinated by the SLT.

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

The Acceptable Use Agreement (Appendix 3) will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use. Staff must sign and follow the Code of Conduct annually; this is coordinated by the member of staff with responsibility for E-Safety. (Appendix 5).

When accessing the Learning Platform from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

Staff must sign the relevant form if they are to remove any school equipment from the school site (Appendix 6) and it should only be used for Beacon of Light School activities.

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 Principal/Senior Designated Person immediately (using Appendix 9) and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted (DSL).

Educational Use of Videoconferencing and/or Webcams please also refer to the COVID-19 Remote Learning Policy

The Beacon of Light School recognise that videoconferencing and the use of webcams can be a challenging activity but brings a wide range of learning benefits.

All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.

Video conferencing will be restricted to school activities in the interests of education and learning or in the interests of safeguarding and pupil welfare.

If you are required to attend virtual meeting meetings this must be first authorised by a member of the SLT

• Please wear clothes which you would normally wear to school

• The meeting should take place in a quiet and private area of your home to maintain confidentiality

• Please ensure the background you are sitting in front of is as plain as possible and does not reveal to the members the contents of you home

• Please ensure that the meeting is conducted in an area of your home which will not be needed by any other members of your family for the duration of the meeting, such as your children

• Please ensure you wear you staff ID lanyard during the meeting

If you are concerned about your capacity to participate in a virtual meeting, please contact the SLT

Users

Users Parents/carers consent will be obtained prior to pupils taking part in videoconferencing activities.

Pupils will ask permission from a member of staff before making or answering a videoconference call or message while on the school site.

Videoconferencing will be supervised appropriately, according to the pupil's age and ability.

Video conferencing will take place via official and approved communication channels following a robust risk assessment.

Only key administrators will be given access to videoconferencing administration areas or remote-control pages.

The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.

If third party materials are included, we will check that recording is permitted to avoid infringing the third party intellectual property rights.

We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the pupils.

Conducting Videoconference from home Please also refer to the COVID-19 Remote Learning Policy

In exceptional circumstances it may be necessary to conduct a video conference from home. The following guidance needs to be followed:

If recording videos or livestreaming lessons, make sure to film in a neutral area where nothing personal or inappropriate can be seen or heard in the background. Staff must be appropriately dressed

If communicating with students online, make sure the platform you are using is suitable for their age group. Also check the privacy settings. Staff must only use the school approved platform for the conference.

Set up school accounts for any online platforms you use. Teachers must never use personal accounts. This also applies to communication via email.

There needs to be a minimum of two staff on each call or conference.

Staff must wear their school lanyard.

Language must be professional and appropriate; this will also include your family members in the background.

Get written consent from parents or guardians for children to be involved in online lessons. An example consent form can be found.

The Beacon of Light School set out clearly when it is and isn't appropriate to contact children at home in the Mobile Phone and Social Media Policies.

If conducting a video conference prior permission needs to be gained from the Principle of the Beacon of Light.

If it is appropriate to communicate with a child on an individual basis – for example, to give feedback on a piece of work – use parents' or carers' email addresses or phone numbers, when it is safe to do so. Do not conduct 1-2-1 conversations through video conferencing.

Make sure any video calls or phone calls are made from a blocked number so teachers' personal contact details are not visible.

Staff must keep calls to a reasonable length so families can get on with their day.

Schools should check that everyone is able to contact the nominated child protection lead and deputy if they have any concerns about a child. This child protection lead should keep a note of any contact numbers they may need while the school is closed, for example, children's social care and the local police.

Talk to children regularly about the benefits and risks of the online world and give them space to ask questions.

Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements (Appendix 4) 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 e-mail 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.

School should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements 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/education setting or other establishment.

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 need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

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 have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.

- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.

- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

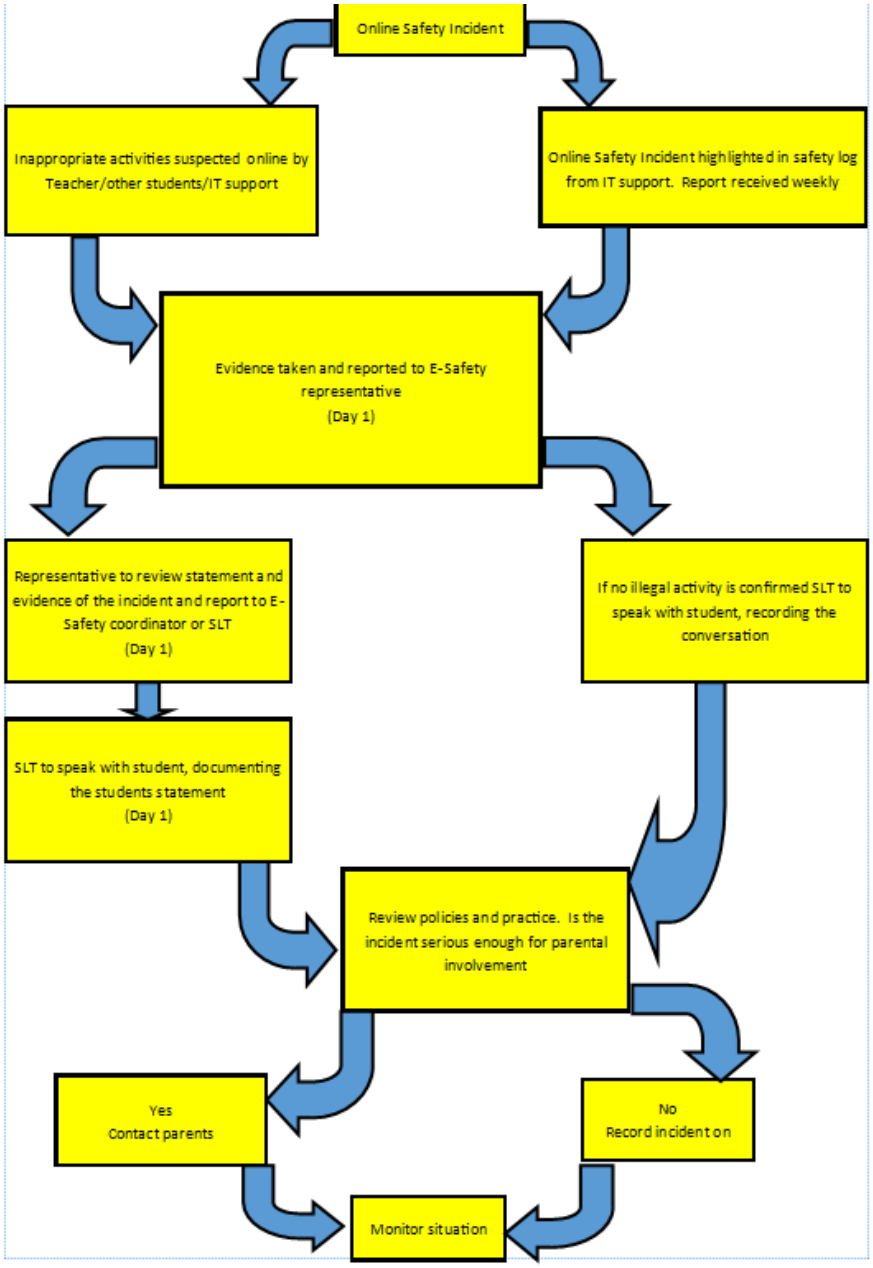
- The student's placement within The Beacon of Light School could be ended.

In the event that 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. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. 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 for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

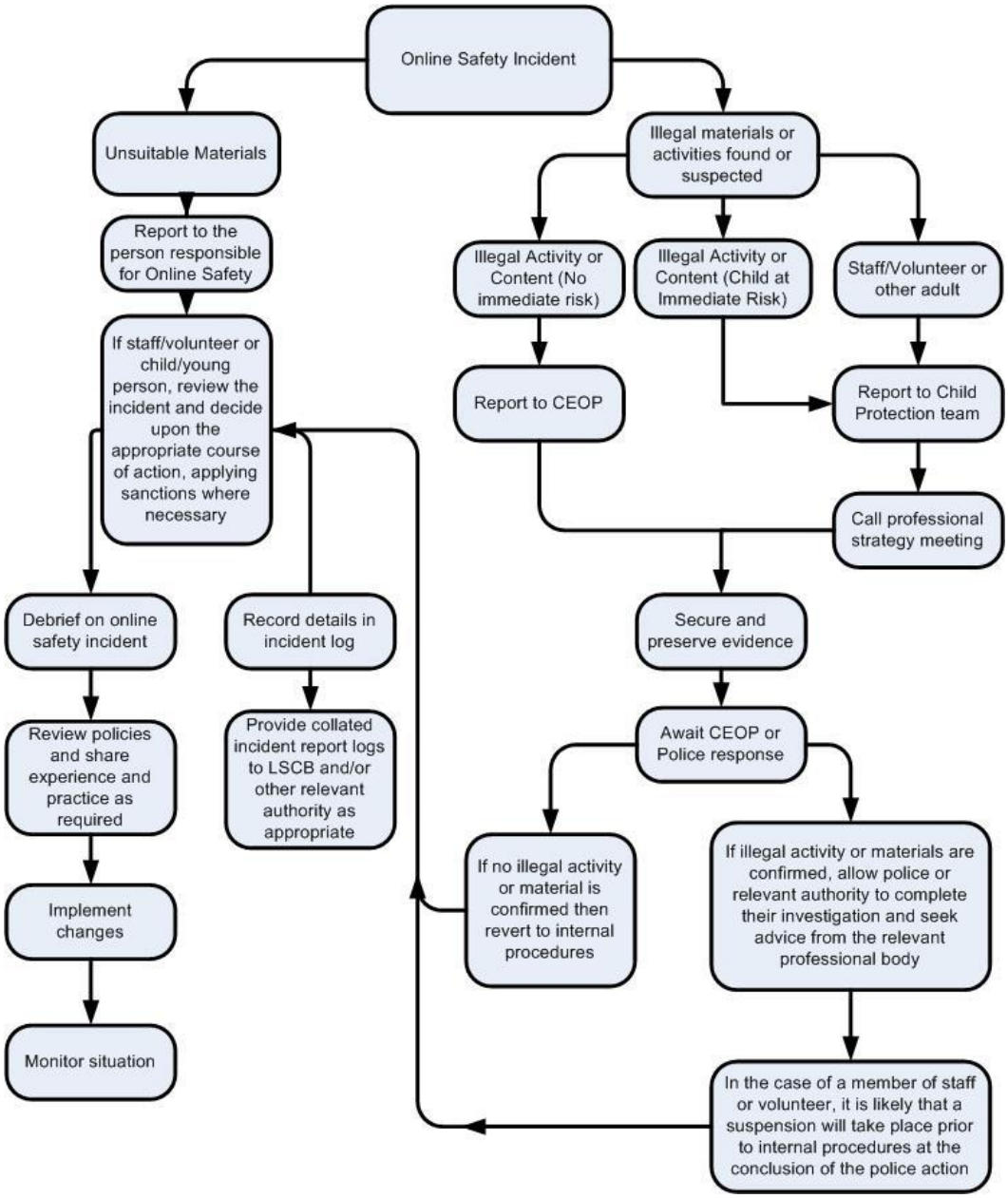
Responding to incidents of misuse:

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). See flow chart on the next page. The timescale for action is shown below.



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, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police. It may also be necessary to inform the LADO.



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:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- 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.

- 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).

- 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).

- 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 of 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.

Appendix 1 Trustees Report

E-Safety Trustee Report

Overview

Type of Incident	Term 1	Term 2	Term 3	Percentage of Incident	Staff Comment
Cyber bullying/ Harassment					
Deliberately bypassing security					
Accessing unsuitable content					
Racist, sexist or homophobic material					
Radicalisation or extremism					
Material of a Sexual Nature					
Other					

Strengths

Areas For Development

Appendix 2

Secure transfer of data and access out of school

The Beacon of Light School recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location

- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school

- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and

- Care should be taken if data is taken or transferred to another country, particularly outside Europe.

Appendix 3

Beacon of Light School – Staff/Volunteers Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone.

These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology.

I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school as outlined in Staff Behaviour Policy (sections 17 & 18 referring to use of school equipment, communication systems and social networking).
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will not allow a student to access a laptop/PC which I am already logged into with my personal staff user/password account
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will record any conversation with parents where safeguarding issues have been identified.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to

do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policy (see Staff Behaviour Policy)
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I understand the risks attached to using personal email addresses / mobile phones / social networking sites for such communications and will only use professional communication addresses/numbers when communicating with students/parents/carers. Personal devices will only be used in extraordinary situation to ensure the well-being of students.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school / academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Protection Policy and Staff Behaviour policy. Where digital

personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Trustees and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name	
Signed	
Date	

Appendix 4

Beacon of Light School - Student Acceptable Use Agreement

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Beacon of Light School - Student Acceptable Use Agreement Form

This form relates to the student / pupil Acceptable Use Agreement; to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student	
Signed	
Date	
Name of Parent/Carer	
Signed	
Date	

Appendix 5

SAFE USE OF ICT AND OTHER DIGITAL DEVICES STATEMENT

Statement of intent
The Beacon of Light School looks to enable the advantages of a wide range of ICT systems and other digital devices, both in school and outside of school. In doing so, Beacon of Light School has a responsibility to ensure that ICT is used appropriately. Where this policy is breached, this may become a matter for investigation and/or a disciplinary issue. Staff should also be aware that this extends to any inappropriate use of ICT and digital devices outside Beacon of Light School.
This Dos and Don'ts list prescribes the types of behaviours and actions that staff should undertake in order to protect Beacon of Light School and themselves from risk.
It is important that this document is read in conjunction with the following policies and documents:

- Data Breach
- E-Safety

Do

- Ensure that where a login and password is required for access to a system, it is not disclosed to anyone
- Personal use of the school's ICT resources and facilities is undertaken outside core work hours
- Be aware that the school's systems will be monitored and recorded to ensure policy compliance
- Ensure that you comply with the requirements of the Data Protection Act when using personal data
- Seek approval from your Line Manager before taking personal data off the school site
- Ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
- Report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Principal or Safe Guarding Officer as appropriate
- Be aware that a breach of your school's Safe Use of ICT and Other Digital Devices – for School Staff policy will be a disciplinary matter
- Ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
- Ensure that you have signed the 'ACKNOWLEDGEMENT OF RECEIPT OF BEACON OF LIGHT SCHOOL PROPERTY Form' confirming what equipment you have been

allocated and that should your employment cease, all equipment will be returned in working order
- Ensure that you have received adequate training in ICT
- Ensure that your use of ICT conforms to appropriate H&S regulations
- Alert your Line Manager or Safeguarding Officer if you receive inappropriate content via email
- Be aware that the school may intercept emails where it believes that there is inappropriate use
- Alert your Principal if you accidentally access a website with inappropriate content
- Use dedicated school mobile devices when on educational visits – not a personal device
- Ensure that your mobile device is switched off during lessons and meetings
- Report to your Principal or Safeguarding Officer any occasion where a pupil has sought to become your friend through a social networking site
- Follow school procedures for contacting parents and/or pupils. Only contact them via school-based computer systems.

Do not,

- Access or use any systems, resources or equipment without being sure that you have permission to do so
- Share your login and password details with anyone
- Download, upload or install any software or hardware (including USB sticks) without approval from the IT Support Team.
- Use any unsecure removable storage devices to store personal data
- Use school systems for personal financial gain, gambling, political activity or advertising
- Use personal email addresses to communicate with pupils or parents
- Accept friendship requests from pupils or parents – you may be giving them access to personal information and allowing them to contact you inappropriately
- Put information or images online or share them with colleagues, pupils or parents (either on or off site) when the nature of the material may be inappropriate
- Post anything that may be interpreted as inappropriate towards colleagues, pupils, parents or the school
- Accept friendship requests from former pupils within 2 years of leaving or until they reach 18, whichever comes first.
- Utilise social networking sites while at work

I have read, understood and accept the School's Safe Use of ICT and Other Digital Devices – for School Staff policy. I am aware that any breach of this policy may lead to disciplinary action. Depending on the severity of the situation, further action may be taken by the school or appropriate authorities.

Name:……

Signed: ……

Appendix 6

ACKNOWLEDGEMENT OF RECEIPT OF BEACON OF LIGHT SCHOOL PROPERTY

Name:

Date:

Description of Equipment or Property Issued to Employee:

By signing this form, I agree to the following: I am responsible for the equipment or property issued to me; I will use it/them in the manner intended; I will be responsible for any damage done (excluding normal wear and tear); upon separation from the Company, I will return the item(s) issued to me in proper working order (excluding normal wear & tear); I will replace any items issued to me that are damaged or lost at my expense; I authorize a payroll deduction to cover the replacement cost of any item issued to me that is not returned for whatever reason, or is not returned in good working order.

Employee Signature: _____

Date: _____

Manager Signature: _____

Date: _____

Details of equipment returned:

_____

_

_____

Manager Signature: _____

Date: _____

Appendix 7

Beacon of Light School - E-Safety Code of Conduct

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc., for school purposes.
- I will not download or install software on school technologies
- I will only log on to the school network/ learning platform with my own username and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Appendix 8 In the event to a school closure

Prior to closure

Principal

- Follow closure directive issued from Government/Police/other relevant organisation
- Inform Chair of Trustees about school closure
- Inform Trustees of closure
- Meet with SLT (this may be in person or via telephone call).
- Discuss protocol and individual responsibilities.
- Notify all staff of closure as soon as possible with expectations of home working, via staff briefing if still in school or via staff school email group
- Guidance issued to staff around expectations of working from home.
- Notify Foundation of Light communications manager of closure for website and Twitter updates.

School Staff

- All staff to respond, either in person or via email, that they are aware of the closure and expectations of home working.
- Staff to take homework laptop. Arrangements to be made to ensure part-time colleagues laptops are delivered home
- Text2Parents and letters sent out via admin to notify parents/carers of school closure
- All Tutors to access school cloud-based isams links from home for student contact details. Paper copies can also be provided where requested.
- Phone calls/emails to be made by each tutor to tutee parents/carers informing of closure, in case texts/letters did not reach home. All calls made from personal/private numbers to be prefixed by 141 to safeguard staff, using script provided (Appendix 4)
- Staff to advise parents/carers to listen to national/local news and access social media for further updates on duration of school closure
- All Tutors to log on Data Dashboard ('school closure' tab) as to which parents/carers have received the message
- All staff to prepare own school laptop to take home for home working. Full-time staff to coordinate and deliver part-time staff laptops

Deputy Principal (Behaviour, Attitude and Personal Development)

- to notify commissioning schools of closure
- to notify student/trainee staff working with school
- to contact external agencies expecting to conduct scheduled meetings in school
- to be the point of contact during closure for Pastoral/SEND/Safeguarding concerns

Deputy Principal (Quality of Education)

- to cancel offsite bookings taking place during enforced closure
- to contact Beacon of Light reception staff to inform them of school closure and redirect callers/visitors to communicate via school email address
- to coordinate Curriculum Leads to prepare subject work packs for expected closure duration
- to collate subject work packs and send to admin
- to prepare covering letter, parent supervision information and amended timetable, explaining expectation for students to complete work at home and return to school once reopened
- to be the point of contact during closure for teaching, learning and assessment issues
- to email closure timetable for Virtual Learning Zone to staff (Appendix 5)

Prior to closure

Reception and Admin

- to contact catering company to inform of school closure and therefore no catering required
- to contact commissioning schools and taxi companies to inform of school closure
- to post work packs out to students with covering letter included

During closure

All staff

- to check emails daily as per staff Code of Conduct Policy
- to be available for tuition contact during dedicated timetabled teaching slot
- to ensure all communication with staff during closure, where possible, is made via school email group.
- all emergency/confidential contact during closure is to be undertaken via line management structure
- to ensure knowledge is updated with current local/national/international news regarding the closure. Recommended website: www.bbc.co.uk
- to ensure no comments are made relating to school closure on social media or other media sources

Principal

- to liaise with DfE/Government re reopening directives
- ensure all information and directives regarding school closure is communicated to staff regularly and in a timely manner via school email group
- to meet with SLT daily to discuss closure situation

Following closure

Principal

- to contact all staff via school email group to communicate reopening date

All staff

- Once school reopening date is confirmed, Text2Parents sent out via admin from home to notify parents/carers of school reopening date
- The day before school reopens, tutors are to contact parents/carers to ensure they have received the message. All calls made from personal/private numbers to be prefixed by 141 to safeguard staff, using script provided (Appendix 4)
- All Tutors to log on Data Dashboard ('school closure' tab) as to which parents/carers have received the message
- All staff to respond, either in person or via email, that they are aware of the reopening date

Appendix 9

E-Safety Incident Report Form

All incidents should be reported to the ICT coordinator.

Date: _____

Name of Person reporting Incident: _____

Pupils Involved: _____

Location of Incident:

Inside of School: _____

Outside of School: _____

Type of Incident

- ☐ Cyber bullying/harassment
- ☐ Deliberately bypassing security
- ☐ Accessing unsuitable content
- ☐ Racist, sexist or homophobic material
- ☐ Radicalisation or extremism
- ☐ Material of a sexual nature
- ☐ Other _____

Nature of Incident:

Deliberate Access:

Created ☐ Viewed ☐ Printed ☐ Shown to others ☐

Distributed ☐

Accidental Access:

Created ☐ Viewed ☐ Printed ☐ Shown to others ☐

Distributed ☐

Description of Incident

_____
_____
_____
_____
_____
_____

Action Taken:

- [ ] Discussion with student
- [ ] Reported to E-Safety Coordinator
- [ ] Parents Informed
- [ ] Safeguarding referral
- [ ] Police informed
- [ ] E-safety policy reviewed