

BEECHVIEW ACADEMY E-SAFETY POLICY

Beechview Academy Policy		Person Group Responsible:	Headteacher
Review Period	Annually	Last review Date:	January 2024

**THE MARLOW
EDUCATION TRUST**

Table of Contents

Page 3	Schedule for Development/Monitoring/Review
Page 3	Scope of the Policy
Page 3	Roles and Responsibilities:
Page 3	Governors
Page 4	Headteacher and Senior Team
Page 4	E-Safety/ICT Coordinator/Designated Person
Page 4	Network/ICT Technician
Page 4	Teaching and Support Staff
Page 5	Child Protection/Safeguarding Designated Person
Page 5	Pupils
Page 5	Parents/Carers
Page 6	Community Users
Page 6	Policy Statements:
Page 6	Education – pupils
Page 6	Education – parents/carers
Page 7	Education – The Wider Community
Page 7	Education & Training – Staff/Volunteers
Page 7	Training – Governors
Page 7	Technical – infrastructure/equipment, filtering and monitoring
Page 8	Bring Your Own Device (BYOD)
Page 9	Use of digital and video images
Page 9	Data Protection
Page 10	Communications
Page 10	Social Media - Protecting Professional Identity
Page 10	Appropriate and Inappropriate Use by Staff or Adults: In the Event of Inappropriate Use
Page 11	Appropriate and Inappropriate Use by Children or Young People: In the Event of Inappropriate Use
Page 12	Responding to incidents of misuse
Page 12	Illegal Incidents
Page 12	Flowchart
Page 13	Other Incidents
Page 14	APPENDIX 1 - Secure transfer of data and access out of school
Pages 15-17	APPENDIX 2 - ACCEPTABLE USE AGREEMENT (Staff/Volunteer)
Pages 18-21	APPENDIX 3 – ACCEPTABLE USE AGREEMENT (Pupil)
Pages 22-23	APPENDIX 4: Online safety incident reporting form

Schedule for Development/Monitoring/Review

Monitoring of the E-Safety Policy will take place at regular intervals.

The Governing Body will receive a report on the implementation of the E-Safety Policy.

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 in January 2025.

Beechview Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys/questionnaires of:
 - pupils
 - parents/carers
 - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers 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.

Beechview Academy 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 Beechview Academy.

Governors

Governors 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 Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the ICT/E-Safety Co-ordinator
- regular monitoring of e-safety incident logs

- regular monitoring of filtering/change control logs
- reporting to relevant Governors

Headteacher and Senior Management Team:

- The Headteacher 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 /ICT/E-Safety Co-ordinator/Designated person.
- The Headteacher and (at least) another member of the Senior Management 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 Headteacher/Senior Management Team are responsible for ensuring that the ICT/E Safety Coordinator/Designated Person and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Management Team 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 Senior Management Team will receive regular monitoring reports from the ICT/E-Safety Co-ordinator/ Designated Senior Person.

E-Safety/ICT Coordinator/Designated Person:

- 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
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Leadership Team

Network/ICT Technician:

The Network/ICT Technician is responsible for ensuring that:

- the school’s technical infrastructure is secure and is not open to misuse or malicious attack.
- the school meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- 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.
- the use of the network/internet/Virtual Learning Environment (VLE)/remote access/email is

- regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ E-Safety Coordinator/Designated Senior Leader for
- investigation/action/sanction.
- monitoring software/systems are implemented and updated as agreed in school policies.

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 Headteacher/E Safety Coordinator/Designated Senior Person for investigation/ action/ sanction.
- all digital communications with pupils/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.
- pupils understand and follow the e-safety and acceptable use agreements.
- 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

Child Protection/Safeguarding Designated Person:

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

Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil Acceptable Use Agreement.
- 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 or other on-line student records.
- their children's personal devices in the school (where this is allowed)

Community Users:

Community Users who access school systems/website/VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils 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/PSHE/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.
- Pupils 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils 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 with any unsuitable material that is found in internet searches.
- 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.

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 InternetDay

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 programme 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.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator/Designated Senior Person (or other nominated person) 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.

Training – Governors:

Governors 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 Governors 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:

Beechview Academy 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
- 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 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 Headteacher.
- 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 limited and the data should always be encrypted and password protected.
 - ✓ 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.

- 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.
- Pupils 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 pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for cyber bullying 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 pupils 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.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' 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 pupils are published on the school website.
- Pupils' work can only be published with the permission of the pupil 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 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.
- 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 and is monitored. Users should be aware that email communications are monitored.
- 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 pupils or parents/carers (email, chat, VLE etc.) must be professional in tone and content.
- Pupils 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 pupils 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, cyber bully, 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.

Beechview Academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, 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.

School staff should ensure that:

- No reference should be made in social media to students, 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.

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 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.

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.

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 Headteacher/Designated Person immediately 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.

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 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 with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children 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 email, 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'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 is deemed to have misused technology against another child or adult.

In the event that a child **accidentally** accessed 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.

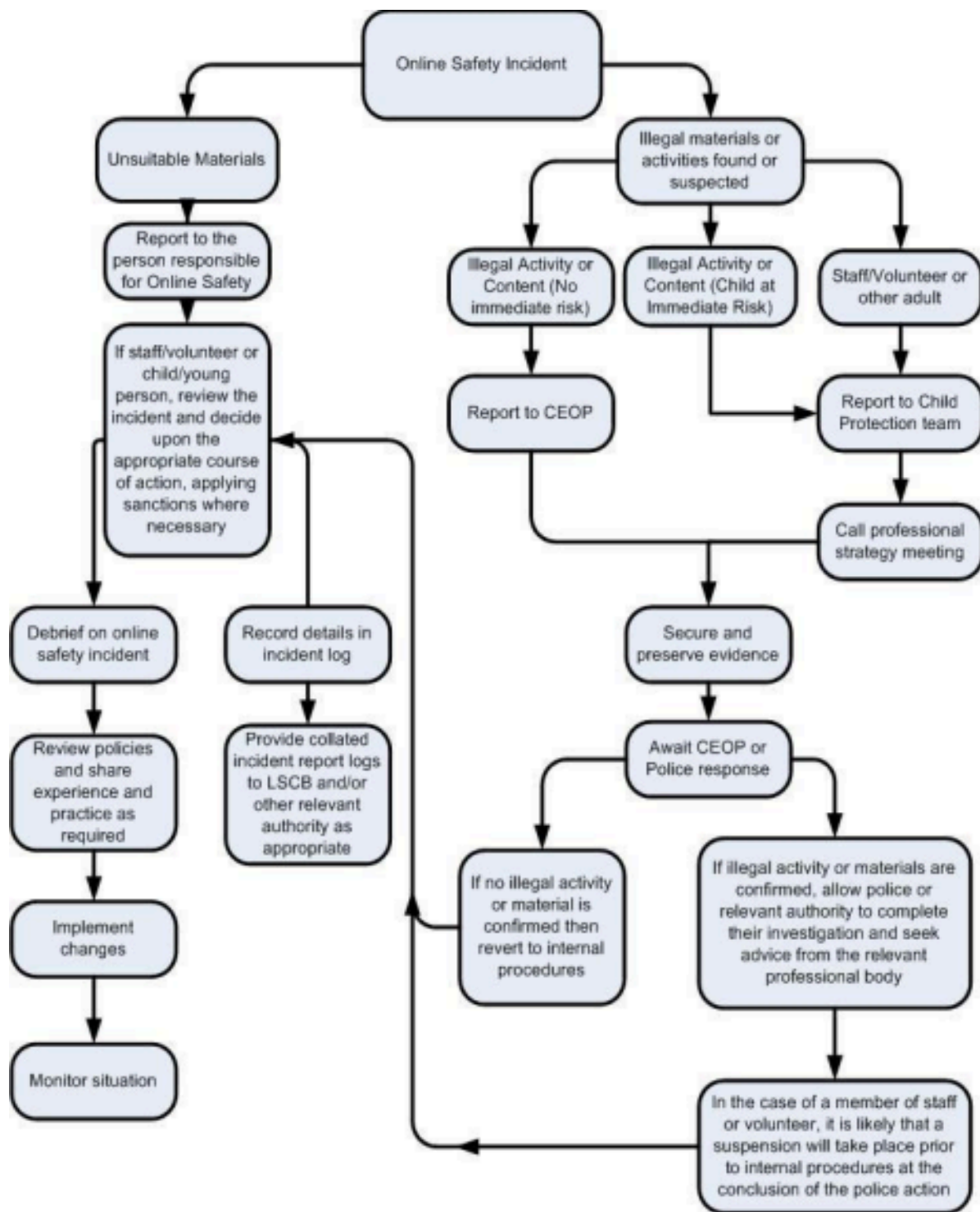
Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this may have legal implications.

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.

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 (see over and appendix) for responding to online safety incidents and report immediately to the police.



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

children 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.

Secure transfer of data and access out of school

Beechview Academy 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.



ACCEPTABLE USE AGREEMENT

(Staff/Volunteer)

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and 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 Internet access 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.
- Beechview Academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- staff are protected from potential risk in their use of ICT in their everyday work.

Beechview Academy will try to ensure that staff and volunteers will have good access to ICT 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.

This policy applies to any device in school. It applies across the whole network and includes WiFi.

Beechview Academy carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, Beechview Academy can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the Internet is closely monitored by the school (BCC/Updata filtering), logs are kept of activity, whether on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how long from which device.

The school email system is provided for educational purposes, where required the school has the ability to access your school email for safeguarding purposes.

Acceptable Use Policy Agreement

I understand that I must use ICT systems at Beechview Academy in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that Beechview Academy will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to Beechview Academy ICT systems (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 Beechview Academy ICT 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.
- 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 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 BeechviewAcademy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with 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 Beechview Academy website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Beechview Academy 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 (PDAs/laptops/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 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 programmes).

- 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 programmes 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 programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school 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 E-Safety Policy, Appendix 3. 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 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 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 Beechview Academy:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Beechview Academy
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors 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 ICT 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 _____

Once signed, please retain a copy for your reference and return the original to the main office at Beechview Academy on the same day as issued



ACCEPTABLE USE AGREEMENT

(Pupil)

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 Policy is intended to ensure:

- that children and 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 users at risk.

Beechview Academy will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect them to agree to be responsible users.

This policy applies to any device in school. It applies across the whole network and includes Wi-Fi.

Beechview Academy carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, Beechview Academy can read the information and remove inappropriate content or prevent access to the material.

Your activity on the Internet is closely monitored by the school; logs are kept of activity, whether on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how long from which device.

Acceptable Use Policy Agreement

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

For my own personal safety:

- I understand that Beechview Academy will monitor my use of the systems, devices and digital communications.

- I will keep my username and passwords safe and secure – I will not share them, 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 on-line (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 on-line.

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

- I understand Beechview Academy 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 use Beechview Academy systems or devices for on-line gaming, on-line gambling, 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 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 BeechviewAcademy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of BeechviewAcademy:

- 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 will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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 Beechview Academy 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.

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.



**ACCEPTABLE USE AGREEMENT
(Pupil)**

This form relates to the 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 ICT systems.

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

- I use Beechview Academy systems and devices (both in and out of school)
- I use my own devices in Beechview Academy (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of Beechview Academy 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 Pupil (PRINT) _____

Year Group _____

Class Teacher _____

Signed by pupil _____

Date: Academic Year 2023/2024

(Please complete and detach this page and return it to the school office)

APPENDIX 4: Online safety incident reporting form



Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to the Headteacher. You can also complete this [form online using this link](#).

Name of person reporting incident:			
Signature:			
Date you are completing this form:			
Where did the incident take place:	Inside school?		Outside school?
Date of incident(s):			
Time of incident(s):			
Who was involved in the incident(s)?	Full names and/or contact details		
Children/young people			
Staff member(s)			
Parent(s)/carer(s)			
Other, please specify			

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Thank you for completing and submitting this form