BIRKENHEAD HIGH SCHOOL ACADEMY
ONLINE SAFETY POLICY

Background

This policy seeks to formalise the management of E-safety risks, incidents, and education within the school. It should be read in conjunction with the school *Safeguarding and Child Protection Policy*, the *Safeguarding Procedures* (which incorporate the staff *Code of Conduct*), and the *Anti-Bullying Policy*. These detail the steps that should be taken in any safeguarding issue whether it is mediated by technology or not.

While many of the risks around E-safety will be familiar, modern technologies have created a landscape of challenges and dangers that are still constantly changing. The continued development of systems and devices means that school leaders will need to be proactive and pragmatic in dealing with problems and threats as they emerge.

This E-safety Policy applies to all members of the school community including staff, students/pupils, volunteers, parents/carers, and visitors. It applies to the whole school, including the Early Years Foundation Stage.

Safeguarding is a serious matter; at BHSA we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

Principles

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to the student or liability to the school.

For clarity, the e-safety policy uses the following terms unless otherwise stated:

- **Users** - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.
- **Parents** – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.
- **School** – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.
- **Wider school community** – students, all staff, governing body, parents.

This policy is available for anybody to read on the BHSA website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students' ICT Code of Conduct will be sent to students at the beginning of each using Firefly, students must tick to accept they have read the policies.

Aims

E-Safety at BHSA will:

- Be informed by latest research and guidance
- Ensure the highest standards of technological protection are included as part of school networks.
- Relevant to our students
- Addressed through assemblies, form time, PSHE, lessons and E-safeguarding is seen as a responsibility of *all* staff.

- Informative to parents
- Regard E-safety education as an important preparation for life.
- Recognise that pupil and family information is sensitive and private. Data protection is regarded as a high priority.

Practice

Filtering and monitoring

Introduction
When talking about an Internet filter there are two important aspects:

Filtering
This is a pro-active measure to ensure or prevent users, as much as possible, from accessing illegal or inappropriate websites.

We filter Internet activity for two reasons:

- to ensure, as much as possible, that children and young people, and to some extent adults, are not exposed to illegal or inappropriate websites. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- to ensure, as much as possible, that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

Monitoring
This is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

We monitor for assurance

- (as much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.
- As a way of safeguarding.

All schools within the GDST are centrally provided with their data connections via a dedicated network. All incoming data are screened by an application that provides real-time filtering and protects both networks and users from Internet threats. It prevents a wide range of unwelcome material and malware from being available in schools while at the same time allowing access to educational material from (for example) YouTube. The policy determining filtering is managed centrally, with different levels being applied depending on age group.

The filtering system produces a daily report based on access to specific blocked categories as well as keywords. The report identifies situations where pupils and staff have tried to access sites which may give rise to concern. Monitoring is also undertaken for example, reports can be generated about the types of sites being accessed by users of the system and the number of times they have been requested.

There is also a centrally managed process for scanning email messages between staff and students for inappropriate language and behaviour. If there is an issue the HR department at Trust Office will be alerted and the matter is taken up with the school. Email traffic between pupils is not scanned as a matter of course, but if concerns about contacts between pupils are raised, then a record of messages can be retrieved by GDST IT.

The E-safety Co-ordinator keeps a log of all E-safety incidents in the school and shares this on a regular basis with the senior leadership team and school network manager. She also monitors the implementation of the E-safety Policy and ensures that its provisions are being implemented.

BIRKENHEAD HIGH SCHOOL ACADEMY
ONLINE SAFETY POLICY

A right to privacy?

Everybody has a right to privacy, whether adult or child, but in certain circumstances there is a reduced expectation of privacy. In the context of this guide, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

Managing expectations

It is the expectations of the user that are particularly important; this will include school staff, students and parents/guardians of the students. Consent is not a requirement, however we are required by law (Data Protection Act 1998) to make all reasonable efforts to inform users that we are monitoring them. By making reasonable efforts we believe we are working "with" the students and parents, not just merely telling them.

Summary

- Filtering is different to monitoring.
- Consent is not required.
- Users are informed that we are monitoring their internet use.

Acceptable Use Agreements and authorising internet access

Before using any school IT resource all staff members are required to read and sign an Acceptable Use Agreement (AUA) as part of their contract of employment. Staff have a dedicated log-on which requires them to use a strong password for access to the system. The first time they log-on, an automatic on-screen message reminds them about their responsibilities under the AUA and requires them to acknowledge this. Their response is then logged.

Differing versions of this agreement may be used to match the personal and professional roles of staff members. A copy of the agreement will be given to staff members for their reference. The AUA details how school equipment and connections may be used.

Pupils' Acceptable Use Agreements include E-safety guidance in the form of three age-appropriate leaflets or posters. Although not a legal contract, the agreements do set out what is expected by the school, and this guidance is shared with parents.

A separate register of when pupils were given (and agreed to abide by) the provisions of the agreement is kept for future reference with the pupil's records.

The school will keep a record of all staff and pupils who are granted Internet access through the individual usernames granted. The record will be kept up-to-date. (This will take account of changes such as a member of staff who has left the school or a pupil whose access has been withdrawn.)

Visitors to the school can be given access to the Internet by connecting to Visitor wireless. The filtering and monitoring systems apply as above. Access for visitors is provided under the general terms and conditions of the GDST, which prohibit the sending or receiving of materials which "are offensive, abusive, defamatory, obscene, or menacing" or which are illegal. The visitor signs a disclaimer which outlines restrictions and expectations of use.

Staff use of Equipment and the Internet

The equipment provided for staff is primarily intended to support the teaching and learning of pupils. However, it is unreasonable to deny staff access to the Internet for legitimate personal use (for example to contact a son's or daughter's school). Nevertheless, discretion and the highest professional standards are expected of staff using school equipment.

Expectations are set out in detail in the *Acceptable Use Agreement* and in this policy, but will include:

- Keeping a proper professional distance e. g. not “friending” pupils on social networking sites.
- Being aware of the need for appropriate language and behaviour particularly when using messaging or e-mails.
- Not posting inappropriate material on websites which can be viewed by pupils or parents/carers.

Misuse of school systems

Because the staff *Acceptable Use Agreement* is part of the contract of employment, misuse is a disciplinary matter.

Pupil misuse (for example the sending of bullying messages to another pupil) may result in the withdrawal of facilities or further sanctions in line with the school's disciplinary policy.

Abuse of the systems by visitors will result in the immediate withdrawal of access and possible further action depending on the nature of the misuse.

Technology

BHSA uses a range of devices including PC’s, laptops and Apple devices. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Fortinet Firewall Solution software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, e-Safety Officer and IT Support Team are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Principal.

Email Filtering – we use Microsoft inbuilt filtering software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All staff school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Principal immediately. The Principal will liaise with GDST to ascertain whether a report needs to be made to the Information Commissioner’s Office.

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change quarterly or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Principal if there are any concerns. All visitors’ USB peripherals such as keydrives are to be scanned for viruses before use.

Safe use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; to students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Students are permitted to use the school email system, and as such will be given their own email address. The email address will be their forenamesurname@birkhs.gdst.net eg joannabloggs@birkhs.gdst.net

Photos and videos –All parents/carers must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will be assumed as acceptance.
Social Networking – there are many social networking services available; BHSA is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within BHSA and have been appropriately risk assessed. Should staff wish to use twitter as a platform of communication with students, they must have a BHSA branded account and have informed the e-safety officer. They must not follow students. Should a member of staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Principal for a decision to be made. Any new service will be risk assessed before use is permitted.
 Blogging – used by staff and students in school.
 Twitter – used by the school as a broadcast service (see below).
 Facebook – used by the school as a broadcast service (see below.)

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.
In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use.

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.
Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in her absence the Vice Principal. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Teaching E-safety in School

The school curriculum includes lessons and activities in E-safety for all pupils.
The intention is to develop pupils' **awareness**, **resilience**, and **skills** in the wider electronic world. Pupils will explore issues such as:

- **Persuasion and reliability** (internet scams, phishing, unreliable information, radicalisation and extremism, etc.);
- **Personal information and safety** (sexting, social network information, personal images, etc.);
- **Sexual exploitation** (grooming, sexting, "offender not present" activities, etc.);
- **Online bullying** (text abuse, "trolling", etc.).

The activities are differentiated with regard to age.

The curriculum is varied and may comprise:

- staff-led skills sessions (e.g. How to configure *Facebook* privacy settings)
- whole-school assemblies led by older pupils, and other examples of peer mentoring
- discussion groups
- 'Safer Internet Day' activities
- formal lessons.

The teaching covers not only what the problems are, but how to deal with and avoid them. Wherever possible, we engage older pupils to share their experiences and advise others about personal safety and responsibility online.

These activities and lessons form part of the Computing/IT and PSHE schemes of work.

The E-safety Co-ordinator keeps up to date on emerging trends and alters the guidance and focus of the curriculum appropriately.

Guidance to pupils on using e-mail and other messaging systems

- When using the school system, pupils may only use approved email accounts.
- Pupils must immediately tell a member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

As part of the *Acceptable Use Agreement*, pupils undertake never to send hurtful or damaging messages to anyone in the school community regardless of the ownership of the device that the message is sent or received on. Older students are reminded that the sending of abusive messages is illegal.

Particular concerns

Inappropriate material appearing on school computers

- Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting. They are encouraged to talk to their teacher. The teacher should report the incident to the E-safety Co-ordinator who will log the problem and liaise with the network manager to adjust filtering settings.

Abusive messages on school computers

- Pupils who receive abusive messages over school systems will be supported, and advised not to delete messages. The E-safety Co-ordinator will be informed and an investigation begun initially with the help of the Network Manager.

Pupil reporting outside school

- Pupils are taught that if something worries them, or if they think a situation is getting out of hand, that as well as talking to a teacher they can share this with their parents, and consider using the online **Report CEOP** button to make a report and ask for help.

Mobile data

- Whilst access to the internet using the GDST network will be subject to filtering and monitoring, the school is aware that many children will have unlimited and unrestricted access to the internet, for instance via 3G and 4G personal devices, both whilst in school and outside school. However, the AUA the pupils sign and the school's e-safety education cover the responsible use of IT in any situation, whether using the school's networks or not.

Staff training and updates

- All staff will have E-safety training included as part of their safeguarding induction to the school.
- All staff receive regular training in safeguarding pupils. E-safety is included as part of this. Staff members receive training in specific elements of E-safeguarding (e. g. self-harm) and a broader update at least once a year.
- E-safety incidents and concerns are a standing item at staff briefings where appropriate.

Reporting of E-safety concerns

The school takes reports concerning E-safety very seriously. The action taken depends on the nature of the concern raised.

All incidents that come to the attention of school staff should be notified to the E-safety Co-ordinator.

The E-safety Co-ordinator will ensure that pupils, parents, volunteers, and staff understand that they can contact them with concerns at any time.

Any incident that raises wider safeguarding questions will also be communicated to the Designated Safeguarding Lead(s) and action under the *Safeguarding Policy* and *Procedures* will be considered.

Firefly

Advice, guidance, and links are available through the school's VLE, Firefly, for parents/carers and pupils. This advice includes details of how to report a problem to the school, and which members of staff have responsibility for resolving a problem or taking issues further.

Risk Management – Everyday E-safety

Assessing risks

The school will take all reasonable precautions to ensure that users abide by the acceptable use rules and access only appropriate material.

The school cannot be liable for the consequences of staff or pupils deliberately breaking the acceptable use rules which are published for their protection.

Due to the international scale and linked nature of Internet content, it is also not possible to guarantee that unsuitable material will never appear on a computer even when filtering is in place and users abide by the rules.

The school cannot accept liability for material accessed, or any consequences of Internet access.

Staff using IT equipment will mainly be covered by the provisions of the *Display Screen Equipment (DSE, Health and Safety) Regulations* 1992. Guidance, definitions, and requirements can be found on the Health and Safety section of the GDST staff intranet. .

The use of DSE by pupils is not covered by the *Display Screen Equipment Regulations*. However, it is good practice to apply the requirements of the legislation to their workstations thus helping them to develop safe working practices. In particular it is recommended that adjustable seats are provided at pupil workstations and they should be given guidance on appropriate work positions and routines.

If pupils are issued with laptops, tablets, etc. then a risk assessment must be completed and guidance on how to use them given safely. A template risk assessment and pupil advice sheet can be found on the GDST staff intranet Health and Safety Section.

Use of mobile phones and cameras

In order to prevent allegations of inappropriate activities, including against EYFS staff, images of pupils (taken in a school capacity) may only be taken using classroom iPads and/or the academy camera(s) - staff must not use their own personal devices to take images of pupils.

Any images taken on personal devices must be downloaded to school or GDST systems as soon as reasonably possible and the personal copy permanently removed.

Staff must be careful to avoid taking any photos of pupils that could be construed as inappropriate, and any photos that may inadvertently be seen as inappropriate should be destroyed.

Publishing staff & pupil information and photographs

- **The school website**

The contact details on the website should be the school address, email and telephone number. Pupils' personal information will not be published.

The Principal has overall editorial responsibility and ensures that content is accurate and appropriate.

- **Publishing pupils' images and work on the web**
  - **Open / public sites**

Public sites could potentially be used to gather information and the locations of pupils. Written permission to publish photographs and work on websites will have been obtained as part of the contract signed by parents. However, unless there is need to identify a pupil (e. g. to celebrate a prize) the following guidelines should be observed:

1. Pupils' full names will not normally be used on the website or blog, particularly in association with photographs.
2. Photographs published on the website or elsewhere, that include pupils, will be selected carefully. Care will be taken when taking digital/video images that pupils are appropriately dressed.

  - **Closed/ Secure sites**

Pupils' images, video, and work can be made available to parents on secure areas of the web as long as the following measures are adhered to:

1. The parents/carer should have a secure log-on to view the information on their pupils.
2. Parents should be made aware that their child's images may be included in group work viewable by other parents/carers.

Using web sites with pupils

Pupils are often directed to Internet sites as part of their work in school. Many of these sites are very useful and provide facilities such as creating presentations, or working with recorded sounds. In a rapidly changing digital world it is impossible to ask permission from parents for every new site that might be used with pupils or that pupils might discover for themselves. Instead the school will abide by the following principles:

- All sites are filtered via the "Fortinet" system to minimize the risk of inappropriate material being accessed.
- If pupils are asked to make online accounts for access to materials, the minimum of identifiable personal information will be disclosed and only school emails will be used.
- The school will be as open as possible about the sites and software it uses, and it welcomes queries from parents who wish to raise concerns or understand more about the way that IT contributes to education.

It should be noted that because of differing laws (particularly in the USA) terms and conditions of some sites have apparent restrictions which do not apply in the UK. The school takes the view that "restricted" but innocuous sites with useful educational materials will be used unless concerns become evident.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risks will be assessed. It should be understood that potential problems or harm may not emerge until after the adoption of a technology.

The senior management of the school (including the E-safety Co-ordinator) will reassess the suitability of technology and systems over time and check that they remain suitable, secure, and effective.

Handling E-safety complaints

Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the procedures of the school and according to the nature of the complaint.
Any complaint about staff misuse must be referred to the Principal.
For impartiality, investigations into IT misuse by school staff will be carried out by the GDSTs IT Security & Compliance Manager.
Complaints of a child protection nature must be dealt with in accordance with statutory child protection procedures.
Pupils and parents/carers are informed of the school's complaints procedure.

Using non-School Equipment –"Bring Your Own Device"

Under some circumstances, teachers and pupils are now able to use their own equipment in school and connect to the available network. This is normally called "bring your own device" (BYOD).
Whether staff member or pupil, it is made clear to the user that the rules and expectations surrounding online behaviour remain in force regardless of the ownership of the equipment being used – please refer to BHSA's BYOD policy.

Roles and responsibilities

Governing Body	• The governing body is accountable for ensuring that BHSA has effective policies and procedures in place; as such they will: • Review this policy at least annually and in response to any e-safety incident • Ensure that the policy is up to date, covers all aspects of technology use within the school • Ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents. • Appoint one governor to have responsibility for the governance of e-safety at the school who will: • Keep up to date with emerging risks and threats through technology use. • Receive regular updates from the Principal in regards to training, identified risks and any incidents.
Principal – Mrs Mahony	• Has overall responsibility for E-safety provision. • Has overall responsibility for data and data security (SIRO). • Ensures that the school uses the GDST filtered Internet Service. • Ensures that staff receive suitable training to carry out their E-safety roles and to train other colleagues, as relevant. • Is aware of the procedures to be followed in the event of a serious E-safety incident. • Receives regular monitoring reports from the E-safety Co-ordinator / Officer. • Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures (e.g. network manager). • Oversees the staff Acceptable Use arrangements and takes appropriate action over staff who breach them.

E-safety Co-ordinator – Mrs McKenna	• Keeps up to date with latest risks to children whilst using technology; familiarize herself with the latest research and available resources for school and home use. • Review this policy regularly and bring any matters to the attention of the Principal. • Advise the Principal and Governing body on all e-safety matters. • Takes day to day responsibility for E-safety issues. • Promotes an awareness and commitment to e-safeguarding throughout the school community. • Ensures that E-safety education is embedded across the curriculum. • Liaises with school IT technical staff. • Facilitates training and advice for all staff. • Is the main point of contact for pupils, staff, volunteers and parents who have E-safety concerns. • Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident. • Ensures that an E-safety incident log is kept up to date. • Communicates regularly with SLT to discuss current issues, review incident logs and filtering. • Liaises with relevant agencies. • Ensures that staff and pupils are regularly updated in E-safety issues and legislation, and are aware of the potential for serious child protection issues that arise from (for example): o sharing of personal data o access to illegal/inappropriate materials o inappropriate on-line contact with adults/strangers o cyber-bullying o sexting
Computing Curriculum Leader	• Oversees the delivery of the E-safety element of the Computing curriculum. • Liaises regularly with the E-safety coordinator.
Network Manager/technician	• The IT technical infrastructure is secure to include a minimum: o Anti-virus is fit-for-purpose, up to date and applied to all capable devices o Windows (or other operating system) updates are regularly monitored and devices updated as appropriate o Any e-safety technical solutions such as Internet filtering are operating correctly o Filtering levels are applied appropriately • Reports any E-safety related issues that arise, to the E-safety co-ordinator. • Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • Ensures that provision exists for misuse detection and malicious attack

	(e.g. keeping virus protection up to date). • Ensures the security of the school ICT system. • Ensures that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • Ensures that the policy on web-filtering is applied and updated on a regular basis. • Ensures that GDST IT Department is informed of issues relating to filtering applied by the Trust. • Keeps up to date with the school's E-safety policy and technical information in order to carry out the E-safety role effectively and to inform and update others as relevant. • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Keeps up-to-date documentation of the school's E-security and technical procedures. • Keeps an up to date record of those granted access to school systems.
Data Manager	• Ensures that the school is compliant with all statutory requirements surrounding the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the *Data Protection Act* 1998. • Ensures that GDST guidance and policies on the handling of information are implemented. (Guidance is available on the GDST staff intranet).
Teachers	• Embed E-safety issues in all aspects of the curriculum and other school activities. • Supervise, guide and monitor pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant). • Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• Read, understand and help promote the school's E-safety policies and guidance – if anything is not understood it should be brought to the attention of the Principal • Are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices, monitor their use, and implement current school policies with regard to these devices. • Report any suspected misuse or problem to the E-safety coordinator or in her absence the Vice Principal. • Maintain an awareness of current E-safety issues and guidance, e. g. through CPD. • Model safe, responsible and professional behaviours in their own use of technology. • Ensure that any digital communications with pupils are on a professional level and only through school-based systems, never

	through personal mechanisms, e.g. email, text, mobile phones etc. • Ensure that all data about pupils and families is handled and stored in line with the principles outlined in the Staff AUP.
External groups	• Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.

All Students
The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy. E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers
Parents play the most important role in the development of their children; as such BHSA will endeavour to support parents, where possible, to ensure that they have the skills and knowledge they need to ensure the safety of children when using the internet. Through parent forums, school newsletters the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered. Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Communicating the Policy

Introducing the E-safety policy to children

- Versions of the E-safety/Acceptable Use rules are posted in all networked rooms and discussed with pupils as needed. The aim is to keep the policy familiar and fresh for pupils rather than treated as something which is only referred to at odd times.
- Students are sent both the acceptable Use policy and E-safety policy via Firefly at the start of the academic year.
- Pupils are made aware that network and Internet use is monitored.

Staff and the E-safety policy

- All staff will be given a copy of the E-safety Policy and its importance explained.
- They signed a copy of the Staff Acceptable Use agreement as part of the contract of employment.
- Staff should be aware that internet traffic and email can be monitored and traced to the individual user. Because of this, discretion and professional conduct are essential.

Communicating E-safety information to parents

- The school's VLE, Firefly gives information on E-safety and how the school can help.
- E-safety advice will be included as a regular feature in newsletters and as part of the ongoing dialogue between home and school.

- The school holds E-safety events to brief parents/carers about E-safety developments and policies; possibly as part of events such as ‘Safer Internet Day’.
- Wider information events for parents/carers will have E-safety items included in the programme.

Monitoring and evaluation

The E-safety officer will monitor e-safety and the effectiveness of the E-Safety Policy. The E-Safety policy will be reviewed annually or earlier in response to specific E-safety cases.