ONLINE SAFETY POLICY

Last Updated	July 2023
Approved by the Governing Body	To Be Approved
Date to Review	2023-24

Online Safety Policy

Context

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, hark; for example making, sending and receiving explicit images, or online.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in The Acorns School are bound. The school online safety policy will help to ensure safe and appropriate use. The development and implementation of the policy will involve all the stakeholders in a child's education. The Acorns School has robust safeguarding procedures in place and understands that online safety is an integral part of keeping children safe. Keeping Children Safe in Education 2022.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Many of these risks reflect situations in the off-line world and it is essential that this online policy is used in conjunction with other school policies (eg. Behaviour, including anti-bullying, and safeguarding/child protection policies).

The school will demonstrate that it has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected, to manage and reduce these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Online safety encompasses not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- Online safety concerns safeguarding children and young people in the digital world.
- Online safety emphasises learning to understand and use new technologies in a positive way.
- Online safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- Online safety is concerned with supporting children and young people to develop

safer online behaviours both in and out of school.

Some of the material on the internet is published for an adult audience and can include violent and adult content. Information on weapons, crime, racism, extremism and radicalisation may also be unsuitable for children and young people to access. Pupils need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Schools have a duty of care to enable pupils to use on-line systems safely.

The Acorns School needs to protect itself from legal challenge and ensure that staff work within the boundaries of professional behaviour. The law is catching up with internet developments: for example it is an offence to use email, text or instant messaging (IM) to 'groom' children.

It is the responsibility of the school to make it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised" and ensure an Acceptable Use Policy is in place. Online safety training is an essential element of staff induction and part of an ongoing CPD programme.

The rapid development and accessibility of the internet and new technologies such as personal publishing and social networking means that online safety is an ever growing and changing area of interest and concern. The school's online safety policy reflects this by keeping abreast of the vast changes taking place around us.

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

* This policy runs in conjunction with the 'Social Networking Sites and Social Media Policy'.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Mrs Sharon Bennet is the nominated Online Safety Governor

The role of the Online Safety Governor will include:

- Liaising with Online Safety Designated person
- Reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Designated person
- The leadership team members are responsible for ensuring that the Online Safety Person and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Online Safety Designated person:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place, including recording of incidents on CPOMS.
- Organises training and advice for staff.
- Liaises with school ICT technical staff
- Creates a log of incidents to inform future online safety developments,
- Liaises with Online Safety Governor to discuss current issues
- Attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

ICT Technician:

The ICT Technician is responsible for ensuring:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- The school meets the online safety technical requirements outlined in the school's Acceptable Usage Policy and any relevant Local Authority Online Safety guidance
- Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- The school's filtering procedure is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- They keep up to date with e-safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- The use of the network / remote access / Teams is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Designated person for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school procedures.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Online Safety Designated person / SLT for investigation / action / sanction via Technical Services / record on CPOMS if appropriate.
- Digital communications with pupils (email / Teams) should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school online safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils 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

Safeguarding Team

Should be trained in online safety issues and be aware of the potential for serious child protection 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
- Online bullying
- Online materials related to extremism and radicalisation

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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 school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and online bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online 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 therefore take every opportunity to help parents understand these issues through parents' newsletters, letters, website / Text and information about national / local online safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy.

Policy Statements

Education – How pupils are taught to keep themselves safe

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 online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks including exploitation and extremism and build their resilience to these risks.

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of PSHE / form time and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- 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 helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, school website,
- Reviews

Education & Training – Staff

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

- Online safety training will be made available to staff.

- Staff are familiar with the guidance related to Online Safety in Keeping children safe in education 2022
- All new staff should receive online safety training ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Online Safety Designated person will organise the provision of advice / guidance / training to individuals as required

Training – Governors

- Governors should take part in online safety training.

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 online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Technician.
- All users will be provided with a username and password and an up to date record of users and their usernames will be kept.
- The "administrator" for passwords for the school ICT system, will be available to the Headteacher and Online Safety Designated person.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the Technicians needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher and/or the Online Safety Designated person.
- Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher or Online Safety Designated person.
- An appropriate system is in place for users to report any actual / potential online safety incident.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the internet, eg. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technicians 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.
- 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 will not be permitted to use their mobile phone in class unless permission has been granted in advance from the Headteacher.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. 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 eg. on social networking sites.

- Staff 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 pupils 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.

- Parents or carers will have the option to opt in for any photographs of pupils which are to be used for educational or marketing purposes.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed

- Processed for limited purposes

- Adequate, relevant and not excessive

- Accurate

- Kept no longer than is necessary

- Processed in accordance with the data subject's rights

- Secure

- Only transferred to others with adequate protection.

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.

Communications

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. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg. by remote access).
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, Teams etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Web-based technologies

- The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.
- Use of email enables improved communication and facilitates the sharing of data and resources.

Procedures for use of the internet and email

- Users must access the Internet and e-mail using their own account and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's e-mail account. If you feel your account details are known by others you should change your password immediately.

- The Internet and e-mail must be used in a reasonable manner adhering to the professional judgment of the supervising member of school staff.

- Pupils must be supervised at all times when using the Internet and e-mail in school.

- Procedures for safe Internet use and sanctions are applicable if rules are broken.

- Internet and e-mail filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.

- Internet and e-mail use will be monitored regularly in accordance with the Data Protection Act 2018.

- Users must be careful when they disclose any information of a personal nature in an e- mail or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.

- All e-mails sent should be courteous and the formality and tone of the language used appropriate to the reader. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- Bullying, harassment or abuse of any kind via e-mail will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- If users are bullied, or offensive e-mails are received, this must be reported immediately to a trusted adult or member of staff within the service / establishment. emails received should not be deleted, but kept for investigation purposes.

- Copyright must not be broken.

File transfer:
Files may be taken home or brought into school by pupils by using One Drive.

Procedures to ensure safety of Broughton High School website

- All content and images must be approved before being uploaded onto the website prior to it being published.

- The website is checked regularly to ensure that no material has been inadvertently posted, which might put pupils or staff at risk.

- Copyright and intellectual property rights are respected.

- Permission is obtained via the admissions pack from parents or carers before any images of pupils can be uploaded onto the website.

- When photographs to be used on the website are saved, names of individuals should not be used as file names.

Procedures for using mobile phones, digital and other devices

- The school is NOT responsible for pupils' personal mobile technology damaged, lost or stolen. Items are brought to school at your own risk.
- If a mobile phone, or any other digital device needs to be brought into school, it should be switched off at all times and stored at reception.
- If a mobile phone or another device is activated in school when not directed by the teacher as part of a lesson, it will be confiscated immediately, recorded and handed in at Pupil reception. A sanction will apply.
- Staff will not copy/distribute/view images on any pupils' personal mobile device.

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Governing Body / Governors' Access and Support Committee on:	- awaiting approval
The implementation of this online safety policy will be monitored by:	SLT
Monitoring will take place at regular intervals:	annually
The Governing Body / Governors Sub Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	annually
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	September 2024

Concluding statement:

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology at The Acorns School. It may be that staff /pupils might wish to use an emerging technology for which there are currently no procedures in place. The use of emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy update