CREATING A CLIMATE FOR GREAT LEARNING,
SUCCESS AND OPPORTUNITY

# Online Safety Policy

## April 2022

**Responsible Officers:** Designated Safeguarding Lead, Business Manager and Head of IT Services

**Approved by Full Governing Body on:** 29th June 2022

**Policy Aims**

- The purpose of Benton Park School online safety policy is to:
    - Safeguard and protect all members of Benton Park School community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

**The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2021.

**Policy Scope**

At Benton Park School we want to ensure that all members of our community are safe and responsible users of technology. We recognise the educational and social value of technology used in a responsible and positive way. We also recognise our responsibility to support young people and staff to manage risks when using technology.

Information and Communications Technology covers a wide range of resources, including web based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Microsoft Teams
- Mobile/ Smart phones with text, video and/ or web functionality
- Making /receiving phone calls via their mobile phones
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Online shopping

This online safety policy recognises the commitment of our school to e-safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep students safe when using technology. We believe the whole school community can

benefit from the opportunities provided by the Internet and other technologies used in everyday life. The e-safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks, whilst continuing to benefit from the opportunities.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff 'in this policy) as well as students and parents/carers. All parties as outlined are collectively referred to as the 'school community'.

This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop, tablets or mobile phones.

The Person responsible for overseeing all elements of e-safety at Benton Park is Vikki Taylor, Deputy Headteacher.

**Links with other policies and practices**
This policy links with a number of other policies including:

- Anti-bullying policy
- Acceptable Use Policies (AUP)
- Attitude to Learning policy
- Child Protection policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
- Data Protection Policy
- Photographic consent
- Staff Disciplinary Policy

**Monitoring and Review**
Benton Park School will regularly review this policy and revise it in line with any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.

The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.

Any issues identified will be incorporated into the school's action planning.

**Roles and Responsibilities**
We believe that e-safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

**The Senior Leadership Team will:**

- Ensure liaison with the Governors about e-safety
- Develop and promote an e-safety culture within the school community

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- Ensure all members of school staff are aware of the contents of the school's Online Safety Policy and the use of any new technology within school
- Ensure all staff, students, occasional and external users of our school ICT equipment are issued with the relevant Acceptable Use Policy and that new staff have e-safety included as part of their induction procedures
- Ensure that E-safety will be taught as part of the curriculum in an age-appropriate way to all students
- Make this Online Safety Policy available to all parents, carers and others via the school website
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks
- Ensure adequate technical support is in place to maintain a secure ICT system
- Receive and regularly review e-safety incident logs; ensure that the correct procedures are followed should an e-safety incident occur in school and review incidents to see if further action is required
- The Headteacher will take ultimate responsibility for the e-safety of the school community

**Responsibilities of E-Safety Leader:**

- Promote an awareness and commitment to e-safety throughout the school
- Take day to day responsibility for e-safety within the school
- Liaise with technical staff on e-safety issues
- Create and maintain e-safety policies
- Develop an understanding of current e-safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training on e-safety issues
- Ensure that e-safety is promoted to parents and carers
- Ensure that staff and students know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an e-safety incident
- To promote the positive use of modern technologies and the Internet
- To ensure that the school e-safety policy is reviewed

**Responsibilities of all Staff:**

- Read, understand, adhere to and help promote the school's e-safety policies and guidance
- Take responsibility for the security of school systems and the data they use, or have access to
- Develop and maintain an awareness of current e-safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with students is on a professional level and only through school based systems, NEVER through personal email, text, mobile phone, social network or other online medium
- Embed e-safety messages in learning activities where appropriate
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures
- Supervise students carefully when engaged in learning activities involving technology
- Ensure that students are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all e-safety incidents which occur to their line manager

**Responsibilities of Technical Staff:**

- Provide technical support and perspective to the Senior Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures

- Implement appropriate security measures (including password policies and encryption*)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- Ensure appropriate filtering and monitoring systems are in place and that these are kept up to date
- Ensure that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Report any filtering breaches to the Senior Leadership Team, as well as, the school's Internet Service Provider or other services, as appropriate
- Ensure that provision exists for misuse detection and malicious attack
- Report any e-safety-related issues that come to their attention to the e-safety lead
- Ensure that procedures are in place for new starters and leavers to be correctly added to, and removed from, all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the school's ICT equipment
- Ensure appropriate back-up procedures exist, so that critical information and systems can be recovered in the event of a disaster
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

**Responsibilities of Students:**

- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings of other students
- Ensure they respect the rights of other students
- Ensure they respect the values of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all e-safety incidents to appropriate members of staff
- Discuss e-safety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices
- To know, understand and follow school policies regarding bullying (including cyber-bullying)
- Students will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute

**Responsibilities of Parents & Carers:**

- Help and support the school in promoting e-safety
- Read the school AUPs and encourage their children to adhere to them.
- Discuss e-safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology
- To agree to and sign the home-school agreement containing a statement regarding their personal use of social networks in relation to the school
- Parents and carers will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute
- To report concerns to the e-safety lead
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online

- Contribute to the development of the school online safety policies
- Use school systems, such as learning platforms, and other network resources, and social media channels in a safe and appropriate way
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

**Responsibilities of the Governing Body:**

- Read, understand, contribute to and help promote the school's Online Safety policies and guidance, as part of the school's overarching Safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-safety awareness
- To have an overview of how the school IT infrastructure provides safe access to the Internet and the steps the school takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for the school to implement their e-safety strategy

**Responsibilities of Child Protection Officers:**

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate
- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information
- Be aware of and understand the risks to young people from online activities, such as grooming for sexual exploitation, sexting, cyber bullying and others
- Raise awareness of the particular issues which may arise for vulnerable students in the school's approach to e-safety, ensuring that staff know the correct child protection procedures to follow
- Respond appropriately to concerns raised by the monitoring systems in relation to safeguarding
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- Report online safety concerns, as appropriate, to the Senior Leadership Team and Governing Body

**Educating Students about online safety**

Students will be taught about online safety as part of the curriculum:

**All** schools have to teach:

- Relationships and sex education and health education in secondary schools
- We will also cover staying safe online, including but not limited to internet scams, and financial fraud, sharing and using data on the Internet, Phishing and the risk of online gambling and cybercrime
- Through our Aspiration for All programme we cover financial scams and fraud, understanding financial advertising and the inappropriate nature of some of this advertising within this we will also be able to link in to online financial risk.

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

**Awareness and engagement with parents and carers**

- Benton Park School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies
- The school will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parents' evenings and transition events
    - Drawing their attention to the school online safety policy and expectations in newsletters, letters, and on our website
    - Requesting that they read online safety information as part of joining our school, for example, within our home school agreement
    - Requiring them to read the school AUP and discuss its implications with their children

**Access to School Systems**

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords.

Suitable arrangements are in place for regular visitors, governors and temporary staff, who may be granted a temporary login. In addition, there is access to guest Wi-Fi which may be granted to visitors. These are all covered by the relevant Acceptable Use Agreements.

All users are provided with a login appropriate to their key stage or role in school. Students are taught about safe practice in the use of their login and passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

**Passwords**

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, etc.)
- We provide all staff with a unique, individually named user account and password for access to IT equipment, email and information systems available within school
- All students have a unique, individually named user account and password for access to IT equipment and information systems available within school

- All staff and students have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their login details. They must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains a log of all access by users and of their activities, while also using the system in order to track any e-safety incidents
- Passwords should be difficult to guess and must meet the following criteria:
    - Minimum of 8 characters
    - At least 1 number and special character (e.g. punctuation)
    - Contain a mix of uppercase and lowercase characters
    - Password must be changed every 90 days
    - You must not reuse an old password

**Using the Internet**

We provide the Internet to:

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using, the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

**Using Email**

Email is regarded as an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, students and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

Access to school email systems will always take place in accordance with Data Protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of Conduct. All email activity is recorded in line with data protection laws. The school is able to view these records in situations where this is called upon.

The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

School email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the school community will immediately tell Claire Scaife or another designated member of the safeguarding team if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

It is the personal responsibility of the email account holder to keep their password secure.

We require all students who use the Internet and email at Benton Park to follow the school's ICT Acceptable Use Policy. This includes being responsible for:

- Their own username and password and not sharing this with others
- Their behaviour and communication when using the network

- Reporting any unpleasant messages or materials sent to them

School will set clear guidelines about when student-staff communication via email is acceptable.

Under no circumstances will staff contact students, parents or conduct any school business using a personal email address.

Responsible use of personal web mail accounts on school systems is permitted for staff only outside teaching hours.

Users should never open attachments from an untrusted source and any unexpected or suspicious emails should be reported immediately to the IT services team

## 6. Cyber-bullying

### 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHCE) education, assemblies and other subjects where appropriate.

All staff receive training regarding online safety.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police based on the severity of the incident.

### 6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or ask a parent/carer to ensure it is deleted
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also retain devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

**8. Students using mobile devices in school**

Students may bring mobile devices into school, but are not permitted to use them anywhere within the school building at any time. This includes during:

- Lessons – unless specifically given consent by the teacher for educational reasons
- Form group time - unless specifically given consent by the teacher for educational reasons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by students must be in line with the acceptable use agreement

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

**Publishing Content Online**

**School Website**

The school maintains editorial responsibility for any school initiated website or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school website, by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the website is the school address, e-mail and telephone number.

Identities of students are protected at all times. Parents have the option to opt out, so that pictures of individual students are not published on the website. Group photographs do not have student surnames attached.

**Online Material Published Outside the School**

Staff and students are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by students, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of, another student or member of the school community will be considered a breach of school discipline and treated accordingly.

**Using Images, Video & Sound**

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Students are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of students wearing appropriate dress. We ask all parents/carers and/or the students for consent to use the photographs and video of their children to be used (in publications and on websites).

For their own protection, staff or other visitors to school are directed not to use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of students. In the event that this is

necessary, it will be with the permission of a member of the Senior Leadership Team and all photos and/or video must be unloaded onto the school system and deleted off the device at the earliest opportunity.

We are happy for parents to take photographs at school events, but will make them aware that they are for personal use only and if they have taken photographs of children other than their own, they should not be uploaded to social media sites and can be only used for their personal use.

**Social Media Expectations**

- The expectations regarding safe and responsible use of social media applies to all members of Benton Park School community, including but not limited to, staff, students, parents, carers, governors, volunteers, extended family members
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger
- All members of Benton Park School community are expected to engage in social media in a positive, safe and responsible manner, at all times
- All members of Benton Park School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others
- The school will control student and staff access to social media whilst using school provided devices and systems on site
- The use of social media during school hours for personal use is not permitted
- Concerns regarding the online conduct of any member of Benton Park School community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child Protection policies

**Staff Personal Use of Social Media**

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of Conduct within the AUP
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can
    - Being aware of location sharing services
    - Opting out of public listings on social networking sites
    - Logging out of accounts after use
    - Keeping passwords safe and confidential
    - Ensuring staff do not represent their personal views as that of the school
- Members of staff are encouraged not to identify themselves as employees of Benton Park School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework

- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school
- All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles
- Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher
- Any communication from students and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead

**Students' Personal Use of Social Media**

- Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources
- The school is aware that many popular social media sites state that they are not for children under the age of 13, and as such school will reinforce this message
- Any concerns regarding students' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Students will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
    - To use safe passwords
    - To use social media sites which are appropriate for their age and abilities
    - How to block and report unwanted communications and report concerns both within school and externally

**Official Use of Social Media**

- Benton Park School may now or in the future make use of official social media channels. Examples of such channels are Twitter, Facebook, Snapchat and any other relevant applications identified in the future
- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes
- The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher and Senior Leadership Team
- Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only
- Public communications on behalf of the school will be closely monitored and quality assured
- Official social media use will be conducted in line with existing policies, including: Antibullying, Photographic Consent, Data protection, Confidentiality and Child protection
- All communication on official social media platforms will be clear, transparent and open to scrutiny

- The school reserves the right to remove any comments it feels adversely affect the reputation of the school or any members of the school community. It further reserves the right to block users who continually use any social media channels in a way which damages the reputation of the school and / or causes offence or distress to any member of the school community
- Any complaints relating to school will be dealt with under the Complaints Policy and not by way of social media commentary. Members of the school community will be advised that the use of social media is not the correct vehicle to express complaints or issues surrounding any aspect of the school.
- Parents, carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community
- Parents and carers will be informed of any official social media use with students and written parental consent will be obtained, as required.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

**Staff expectations**

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Sign the school's Acceptable Use Policy which includes guidelines on social media use
    - Be professional at all times and aware that they are an ambassador for the school
    - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school
    - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared
    - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws

    Ensure that they have appropriate written consent before posting images on the official social media channel
    - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so
    - Not engage with any direct or private messaging with current, or past, students, parents and carers
    - Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from students

**Using Other Technologies**

As a school, we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an e-safety point of view.

We will regularly review the e-safety policy to reflect any new technology that we use, or to reflect the use of new technology by students.

Staff or students using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

**11. Training**

All new staff members will receive online safety training as part of their induction

All staff members will receive regular reminders related to their own and students' online safety.

More information about safeguarding training is set out in our child protection and safeguarding policy.

**Dealing with e-Safety Incidents**

In situations where a member of staff is made aware of a serious e-safety incident concerning students or staff, they will inform the e-safety Lead, Child Protection Officer, their line manager or the Headteacher, who will then respond in the most appropriate manner.

Instances of cyberbullying will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognises that staff as well as students may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's e-safety Lead and technical support and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy, then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that student data has been lost. School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

**Dealing with Complaints and Breaches of Conduct by Students**

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the student will work in partnership with staff to resolve any issues arising
- Restorative practice will be used to support the victims
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

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

- Accessing inappropriate or illegal content deliberately
- Deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- Staff using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities would normally be unacceptable;

- Accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- Accessing non-educational websites (e.g. Gaming or shopping websites) during lesson time
- Sharing a username and password with others or allowing another person to login using your account
- Accessing school ICT systems with someone else's username and password
- Deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else