BEAUCHAMPS HIGH SCHOOL.

Beauchamps Drive, Wickford, SS11 8LY
Headteacher: Mathew Harper BA Hons, NPQH

E-Safety Policy

School Policy/Procedure No: 63

Last Reviewed: July 2018 *Last Amended: July 2018* *Next Review: July 2019*

Introduction

At Beauchamps High School we understand the responsibility to educate our students on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is supported by the school's Acceptable Use Agreements for staff, Governors, visitors and students, which they need to sign, and is to protect the interests and safety of the whole school community and the General Data Protection Regulation (GDPR) Policy. It is linked to the following mandatory school policies: Child Protection, Health and Safety, Home–School Agreements, and Behaviour/Student Discipline (including the Anti-Bullying and PSHE policies) and the Staff Discipline and Dismissal Policy.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, potentially damage the reputation of the school and is a possible breach of GDPR. This can make it more difficult for our school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. Both this policy and the Acceptable Use Agreements (for all staff, Governors, visitors and students) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, mobile phones, tablets, webcams, whiteboards, voting systems, digital video equipment, etc), and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players, etc).

Monitoring

IT authorised staff monitor, intercept, access, inspect, record, store and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school IT; for quality control or training purposes; to comply with a Subject Access

Request under the Data Protection Act 1998 and GDPR 2018, or to prevent or detect crime.

IT authorised staff may, without prior notice, access the e-mail, Office 365 account or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by IT authorised staff and comply with the Data Protection Act 1998, GDPR 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2016 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using school IT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school and its internet provider as part of the Regulation of Investigatory Powers Act 2016 (RIPA)

Breaches

A breach or suspected breach of policy by a school employee, contractor or student will result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual, until any investigations have been completed. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the Staff Discipline and Dismissal Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school's Senior Information Risk Owner (SIRO) or E-Safety Co-ordinator – Mr C Carrott. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must be reported to the ICT Strategy Manager.

Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff will be issued with the relevant guidance documents and the E-Safety Acceptable Use Agreement
- Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile IT equipment or removable storage media in unattended vehicles. Where this is not possible, it must be kept locked out of sight
- Staff must always carry portable and mobile IT equipment or removable media as hand luggage, and keep it under their control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.

Managing Digital Communications

- The school gives all staff their own Office 365 account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations or parents are advised to cc. the Subject Leader, HOY or line manager
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- However you access your school Office 365 account (whether directly, through webmail when away from the office or on non-school hardware) all the school policies apply
- The use of personal email accounts for sending, reading or receiving business related e-mail is not permitted unless authorized by the ICT Strategic Manager.

Sending Digital Communications

- It is the responsibility of the account holder to ensure that email/chat communications are directed to the correct recipient and the contents of the communication are appropriate
- Staff must use their own school e-mail account so that they are clearly identified as the originator of a message
- Staff should keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Staff should not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

Receiving Digital Communications

- Staff should check their e-mail and messages regularly, before school, break, lunch and after school
- Staff should never open attachments from an untrusted source; consult the IT Systems Manager first.
- The automatic forwarding and deletion of e-mails is not allowed
- Should staff receive inappropriate emails/messages from colleagues, students or individuals outside the organization, this should be reported to the IT Systems Manager, ICT Strategic Lead or a member of the Senior Leadership Team immediately.

E-mailing personal, sensitive, confidential or classified Information

- Staff should assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided wherever possible

- The use of personal email accounts for sending e-mail containing sensitive information is not permitted.
- Where the conclusion is that e-mail must be used to transmit such data:
    - Obtain express consent from your SLT line manager to provide the information by e-mail
    - The emails must be encrypted or have an encrypted document as an attachment
    - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
    - Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
    - Provide the encryption key or password by a **separate** contact with the recipient(s) – preferably by telephone Do not identify such information in the subject line of any e-mail
    - Request confirmation of safe receipt

Computer viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB, CD) must be checked for any viruses using school provided anti-virus software before using them
- Staff must never interfere with any anti-virus software installed on school IT equipment
- If a machine is not routinely connected to the school network, staff must make provision for regular virus updates through the IT team
- If staff suspect there may be a virus on any school IT equipment, they should stop using the equipment and contact the IT support provider immediately. The IT support provider will advise you what actions to take and be responsible for advising others that need to know

E-Safety - roles and responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-ordinators in this school are Mr D Windeatt and Mr C Carrott who have been designated this role as members of the Senior Leadership Team. It is the role of the E-Safety co-ordinators to keep abreast of current issues and guidance through organisations such ECC, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

E-Safety in the curriculum

IT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the students on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Students are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline or CEOP report abuse button
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the IT curriculum
- Students will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Schools have additional duties under the Counter Terrorism and Securities Act 2015 which requires them to ensure that children are safe from terrorist and extremist material on the internet.

E-Safety skills development for staff and Governors

- Our staff and Governors will receive regular information and training on E-Safety issues
- New staff will receive guidance on the school's Acceptable Use policy as part of their induction
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to promote E-Safety awareness within their curriculum areas
- All staff and Governors will receive GDPR and Safeguarding training annually.

Managing the School E-Safety Messages

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used

Incident reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT by students must be immediately reported as per the school's Behaviour policy. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance by staff must be reported to the ICT Strategy Manager.

Internet access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use at Beauchamps High School is via a monitoring system. Whenever any inappropriate use is detected it will be followed up.

Internet use

- Staff must not post personal, sensitive, confidential or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Names of colleagues, customers or clients or any other confidential information acquired through an employee's work must not be revealed on any social networking site or blog
- On-line gambling or gaming is not allowed

Parental involvement

We believe that it is essential for parents/carers to be fully involved with promoting E-Safety both in and outside of school, and also to be aware of their responsibilities. We regularly consult and discuss E-Safety with parents/carers and seek to promote a wide understanding of the benefits related to IT and associated risks.

- Parents/carers are asked to read through and sign Acceptable Use Agreements on behalf of their child on admission to school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Home School agreement containing the following statement or similar:
  "We will support the school's approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community."

Password security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- Staff must always use their own personal passwords to access computer based services
- Personal passwords must be used each time staff logon. Staff should not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Passwords should be changed whenever there is any indication of possible system or password compromise
- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Personal passwords should only be disclosed to authorised IT support staff when necessary, and never to anyone else, and should be changed once the requirement is finished
- **If a password may have been compromised or has become known to someone else, this must be reported to the Network Support Team.**
- All users must read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users will be provided with an individual network, email, Learning Platform and (where appropriate) Management Information System log-in username.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are required to be aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)
- Staff will be required to change their user password every 90 days

Protecting personal, sensitive, confidential and classified information

- Staff must ensure that any school information accessed from their own PC or removable media equipment is kept secure
- Staff must ensure that screens are locked before moving away from their computer during a normal working day to prevent unauthorised access
- Staff must ensure the accuracy of any personal, sensitive, confidential and classified

formation they disclose or share with others

- Staff must ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Staff must ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Staff must only download personal data from systems if expressly authorised to do so by their manager
- Staff must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Staff must keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information
- Staff must ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/transferring personal, sensitive, confidential or classified information using removable media

- Staff must ensure removable media is purchased with encryption
- Staff must store all removable media securely
- Staff must securely dispose of removable media that may hold personal data
- Staff must encrypt all files containing personal, sensitive, confidential or classified data
- Network Team staff must ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote access

- Staff are responsible for all activity on their Office 365 account and VPN account
- Staff must only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, staff must keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and not disclose them to anyone
- Staff should select PINs to ensure that they are not easily guessed, e.g. do not use house or telephone numbers or choose consecutive or repeated numbers
- Staff should avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- School information and data must be protected at all times, including any printed material produced while using the remote access facility. Particular care must be taken when access is from a non-school environment

Taking of images and film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. They must use the equipment supplied by the school
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

Publishing students' images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent is updated annually through the Data Collection sheet.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

The consent is an **opt in** process, so failure to return a slip will mean that the school does not have permission.

Students' full names will not be published alongside their image.

Storage of images

- Images/ films of children are stored on the school's network
- Students and staff are not permitted to use personal portable media for storage of student images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform

Webcams and CCTV

- The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school.
- Webcams in school are only ever used for specific learning purposes

School IT equipment

As users of IT, staff are responsible for any activity undertaken on the school's IT equipment provided.

- Staff must ensure that all IT equipment used is kept physically secure
- Staff must not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- Personal or sensitive data should not be stored on the local drives of desktop PCs.
- Privately owned IT equipment should not be used on a school network without permission from the IT Systems Manager
- On termination of employment, resignation or transfer, all IT equipment must be returned to the school. Details of all system logons must also be provided so that they can be disabled
- It is the responsibility of staff to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

Telephone services

- Staff may make or receive personal telephone calls provided:
    1. They are infrequent, kept as brief as possible and do not cause annoyance to others
    2. They are not for profit or to premium rate services
    3. They conform to this and other relevant school policies.
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

Portable & mobile IT equipment

This section covers such items as laptops, smart phones and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network or Office 365, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot before starting a journey
- All locally stored data, including diary entries, should be synchronised with the central school network server on a frequent basis
- Staff must ensure portable and mobile IT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the IT Systems Manager, fully licensed and only carried out by ~~your~~ IT support
- In areas where there are likely to be members of the general public, portable or mobile IT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately:

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched off
- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

Systems and access

- Staff are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school IT equipment or their own PC
- Staff must not allow any unauthorised person to use school IT facilities and services that have been provided to them
- Staff must use only their own personal logons, account IDs and passwords and not allow them to be used by anyone else
- Staff must keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information
- Staff should ensure screens are locked before moving away from their computer during a normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Staff must ensure that they logoff from the PC completely when they are going to be away from the computer for a longer period of time
- Staff must not introduce or propagate viruses
- It is imperative that staff do not access, load, store, post or send from school IT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or ECC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on school systems, hardware or used in relation to school business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

The Network Administration Team will adhere to the following guidelines:

Servers

- Newly installed servers holding personal data should be encrypted, therefore password protecting data. SIMs Database Servers installed by SITSS since April 2009 are supplied with encryption software
- Always keep servers in a locked and secure environment
- Limit access rights to ensure the integrity of the standard build
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Back-up tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Back-up tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote back-ups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied
- Ensure that web browsers and other web based applications are operated at a minimum of 128 BIT cipher strength

Social Media Policy

Introduction:
The principles set out in this policy are designed to ensure that the use of social media among the Beauchamps High school community is undertaken responsibly and that the confidentiality and well-being of students, staff and the reputation of the school are safeguarded. It is intended to represent the ever-growing presence of social media in the school community and to encourage safety for all involved within that community.

Scope:
This policy applies to Beauchamps High School students, staff, parents and the wider school community. It covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.

This policy also applies to personal web space such as social networking sites (for example Facebook, Instagram, Snapchat, Twitter), blogs, chatrooms, forums and podcasts and content sharing sites such as YouTube. Since it is impossible to cover all circumstances or emergent forms of social media, the principles set out in this policy should be followed irrespective of the medium.

Related policies:
This policy should be read in conjunction with the following school policies:
E-Safety Policy
Child Protection/Safeguarding Policies
Anti-Bullying Policy
Behaviour Policy
Staff Code of Conduct

Guidelines for staff

- Staff should decline all friend/follow requests from students that they receive in any personal social media accounts. Staff should not accept any contact from a former member of the school if he/she is under the age of 18.
- Staff should not have contact with a student's family members through personal social media if that contact is likely to present a conflict of interests.
- Staff must not take photographs or videos, even for the use of a school social media account, with personal phones or cameras – the school will have equipment available for loan.
- Only named administrators should post updates or photographs on the school's social media platform; other content should be added via these staff.
- Full names of students will not be posted next to a photograph at any time on the official school social networking forums.
- On personal social media accounts, pupils must not be 'tagged' in any photographs or comments.
- Other members of staff must not be 'tagged' in social media accounts without their prior permission.
- When using a hyperlink in any social media, personal or professional, staff are responsible for checking that the content is appropriate before sharing.
- Staff must not discuss personal information about other pupils, staff or parents on social media.
- Staff should check privacy settings carefully and regularly on personal social media accounts.
- Staff must ensure that passwords and logins to all social media accounts are kept secure at all times.
- School email addresses should not be used for setting up personal social media accounts or to communicate through social media.

- Staff must not engage in any activities on social media which may bring Beauchamps High School into disrepute. This includes posting any material which could be considered as offensive, illegal or discriminatory or have links to extremism, terrorism or radicalization.

Note: All data on E-Safety stored in school is only shared in accordance with the school's Privacy Notice (eg other educational establishments, Local Authority, DfE)