Deyes High School

E Safety Policy (including ICT/Social Networking Policy)

Origination	Authorised by	Issue No.	Page 1 of 13	Date
AST	***DHS BOARD***	***1***		***2016/17***

Policy Rationale

The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to provide our learners with Internet access as part of their learning experience. Deyes High School believes that access to the internet must ensure the safeguarding of all learners.

ESafety

ICT SLT:	Mr P Delaney
Network Manager:	Mr M Hoban
DoL ICT:	Mr J Southworth
Safeguarding Officers:	Mr Birch,Mrs Rens, Mrs Wylie, Mrs Haines and Mrs Illingworth
Director of Finance and Operations (Interim):	Mrs A Pope
Safeguarding Governor:	Mr G Hewer

1.1 **Internet use to enhance and extend learning**

- Deyes' internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Clear boundaries will be set for the appropriate use of the internet and digital communications and discussed with staff and pupils.
- Pupils will be educated in the effective use of the Internet in research, how to critically evaluate the materials they read and shown how to validate information before accepting its accuracy.
- We will ensure that the use of Internet derived materials will comply with copyright law.

1.2 **Managing Internet Access**

1.2.1. Information system security

- Deyes' ICT system security will be reviewed regularly
- Virus protection is installed and updated regularly
- The Headteacher reserves the right to view any information stored on the school network.

1.2.2 Email and messaging

- Pupils must immediately tell an adult if they receive an offensive email or message.
- In any email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Attachments should be treated as suspicious and not opened unless the author is known
- The forwarding of chain emails is not allowed.
- Email communication between staff and pupils should only be via your business email address (name@deyeshigh.co.uk) or the VLE, where messages are stored on the Deyes mail server for security purposes.

1.2.3 Published content on the school website

- Any online contact details for staff should be their Deyes High School email address or the school office
- The VLE: each Faculty will take overall editorial responsibility and ensure that published content is accurate and appropriate.

1.2.4 Publishing pupils' images and work

- Photographs that include students will be carefully selected so that individual pupils cannot be identified or their image misused.
- Students' full names will not be used anywhere on the school website, particularly in association with photographs

- Written permission from parents will be obtained before photographs of

students are published

- Work can only be published with the permission of the pupil

1.2.5 Social Networking and personal publishing

Use of Social Media in the School

- Staff are not permitted to access social media websites from the school's computers or other devices at any time unless authorised to do so by a member of the senior leadership team. They may however, use their own computers or other devices while they are in the school to access social media websites outside of school session times (when your contracted hours have been fulfilled) but excessive use of social media which could be considered to interfere with productivity will be considered a disciplinary matter.

Any use of social media made in a professional capacity must not:

- Bring the school into disrepute
- Breach confidentiality
- Breach copyrights of any kind
- Bully, harass or be discriminatory in any way
- Be defamatory or derogatory
- The school appreciates that people will make use of social media in a personal capacity but they must be aware that if they are recognised from their profile as being associated with the school then certain opinions expressed could be considered to damage the reputation of the school, so a statement such as "the opinions expressed here do not necessarily reflect those of my employer" should be clearly stated and it is advisable to omit any references mentioning the school by name or the person by job title. Opinions should, in any case follow the guidelines to not bring the school into disrepute, breach confidentiality, breach copyright or bully, harass or discriminate in any way.

General Considerations

- When using social media staff and others should
- Never share work log-on details or passwords
- Keep personal phone numbers private
- Not give personal email addresses to pupils or parents
- Restrict access to certain groups of people on their social media sites and pages
- Those working with children have a duty of care and therefore are expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and pupils both within the school and outside of it. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties for "cyber bullying" for example or possibly identify theft. Prior to joining the school new employees should check any information they have placed on social media sites and remove any statements that might cause embarrassment or offence.
- Staff should not use personal mobile phones to contact students and should keep any communications transparent and on a professional basis. Where there is any doubt about whether communication between a student/parent and a member of staff is acceptable or unacceptable/appropriate or inappropriate, a member of the senior leadership team should be made aware and they will then decide how to deal with the situation.
- Deyes High School Staff, Trainees and Volunteers must not accept friend invitations or become friends with any students of Deyes High School.
- Personal Facebook accounts should not be used to discuss any matters pertaining to your professional role at Deyes High School.
- It is strongly recommended that personal social networking sites have the highest privacy settings (see appendix 2 for guidance)
- Deyes High will control access to social networking sites from school, and consider how to educate pupils in their safe use. Please see the additional guidance for Facebook.
- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location
- Pupils should be encouraged to reset passwords on a regular basis, to deny access to unknown individuals and block unwanted communication.
- Pupils should only communicate with known friends.

1.2.6 Managing Filtering

- The school will work in partnership with Sefton LA and Becta to ensure that the systems in place to protect our pupils are reviewed and improved
- If staff or pupils discover an unsuitable site, it must be reported to the ESafety Coordinator. (Mr Hoban)
- The Head of ICT and Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.2.7 Managing Videoconferencing

- Digital phone line video conferencing rights and privileges will be monitored and controlled by the Network manager
- Videoconferencing must be appropriately supervised for the pupils' ages.
- The supervising member of staff will make or answer the videoconference call
- IP videoconferencing rights and privileges will be monitored and controlled by the Network manager

1.2.8 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed
- The SLT should note that technologies with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Therefore, pupils are not allowed to use mobile phones in school.
- Pupils should not attempt to access any wireless connection which is not associated with the school.
- The use by students of cameras in mobile phones is not allowed. If a photograph is needed, school digital cameras can be used.

- Staff should not contact students directly with their own mobile phones unless in exceptional circumstances and a member of the SLT has been informed.
- Staff should be vigilant to avoid the receipt of items via Bluetooth whilst in school.

1.2.9 Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

1.3 Policy Decisions

1.3.1 Introducing the E Safety Policy

- All staff must read and sign the 'Staff Code of Conduct for ICT' to allow use of the school ICT resources
- A list of all current staff and pupils granted access to school ICT systems will be maintained
- Pupils must also apply for Internet access individually by agreeing to comply with the Responsible Use Statement on view in all classrooms and the Library.
- Parents/Carers are also asked to sign and return a consent form

1.3.2 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked

  nature of Internet content, it is not possible to guarantee that unsuitable

  material will never appear on a computer connected to the school network.

  Neither the school, nor Sefton LA can accept liability for any material accessed, or any consequences of Internet access.

- The school will annually audit ICT use to establish if the Esafety policy is adequate and that the implementation of the policy is appropriate and

  effective

1.3.3 Handling Complaints

- Complaints of Internet misuse will be dealt with by the network manager and SLT.
- Any complaints about staff misuse must be referred to the Head teacher
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures
- Discussions will be held with the Police or Community Support Officers to establish procedures for handling potentially illegal issues.

1.4 Communicating E-safety

1.4.1 Introducing the E-safety policy to pupils

- E-safety rules will be posted in all rooms where computers are used
- Pupils will be informed that network and internet use will be monitored
- Training in safety will be developed based on the materials provided by the Child Exploitation and Online Protection centre (CEOP) and delivered to pupils via assemblies. Assemblies will take place on an annual basis.

1.4.2 Staff and the E-safety Policy

- All staff will be given the policy and its importance will be explained

- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user
- Staff managing filtering systems and monitoring ICT use will be overseen by the Network manager and work to clear procedures for reporting issues (see appendix)

1.4.3 Enlisting Parents and Carers Support

- Parents' and Carers' attention will be drawn to the school E safety policy, through the prospectus, on the school website and via parent information evenings.

Appendix 1

Staff Procedures for Breaches of the Policy

1) If a teacher finds unacceptable material on a pupil's account or screen:

a. DO NOT PRINT OFF ANY PORNOGRAPHIC MATERIAL

b. Alert the E Safety Coordinator - Mark Hoban

2) If a pupil reports any cyber bullying issue (malicious text, email, messages) to a member of staff:

a. Refer to the relevant Progress Development manager Leader and this will be dealt with via the usual pastoral channels

b. Progress Development Manager should report the incident to the Esafety Coordinator (Mr Mark Hoban).

Deyes High School: Staff Code of Conduct for ICT

To ensure that all members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, all staff are provided with this code of conduct. Members of staff should refer to the school's e safety policy for further information and clarification.

- Staff should understand that it could be a disciplinary offence to use a school ICT system for a purpose not permitted by the policy.
- Staff should appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital camera, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- Staff should understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- Staff Should understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- Staff should respect system security and I will not disclose any password or security information to anyone other that an authorised network manager.
- Staff should not install any software or hardware on the school network.
- Staff should be aware that if the school has provided me with a laptop, or electronic notebook, it has done so to support me in fulfilling my professional responsibilities. It is Staffs' responsibility to back up work completed on this device. Staff are able to install software on their laptop /

notebook which will help them to fulfil their professional duties. In the event of an error occurring with this device it may be necessary to wipe the hard drive and restore the device to its original settings.

- Staff will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely.
- Staff will respect copyright and intellectual property rights.
- Staff will report any instances of concern regarding children's safety to the ESafety Coordinator and the Designated Child Protection Coordinator (MH & FE).
- Staff will ensure that electronic communications with pupils including email, and the VLE are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- Staff should be aware that images and text posted on public sites may be viewed by pupils and their parents. My professional status should not be affected by anything I post in the public domain.
- Staff should promote safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- Staff will not accept students as friends on a personal social networking site.
- Staff should understand that breaches of this Code of Conduct may result in disciplinary action being taken.

Deyes High school may exercise its right to monitor the use of the school's information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Student E-Safety Rules

These E-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It could be a disciplinary offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information including passwords through email, personal publishing, blogs or messaging.

- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- The school ICT systems must not be used for any message or activity which could be considered to be cyber bullying.
- Vandalism or malicious intent to damage the integrity of the school network facilities will be dealt will seriously. This may result in criminal charges.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers receive the E-Safety Rules have been understood and agreed.

Pupil's Agreement

Pupils must read and I understand the school E-Safety Rules.

Pupils must use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.

Pupils will not use the network and Internet for anything which may be considered cyber bullying.

Pupils should understand that network and Internet access may be monitored.

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also

agree that appropriate images and video that include my son/daughter may

be published subject to the school rule that photographs will not be

accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school E-safety rules and give permission for

my son / daughter to access the Internet. I understand that the school will

take all reasonable precautions to ensure that pupils cannot access

inappropriate materials but I appreciate that this is a difficult task.

Appendix 2

Deyes High School staff MUST NOT accept friend invitations or become friends with any student of Deyes High School. **Personal Facebook accounts should not be used to discuss any matters pertaining to your professional role at Deyes High School.**
(Deyes e-safety policy Feb 2012)

Deyes High recognises that 91% of 13-18 year olds use Facebook and a significant proportion of adults have Facebook accounts to enable them to stay in touch with family and friends. This guide is designed to help you protect your own privacy and the reputation of Deyes High School and Deyes High School Staff. This is an additional guide and does not replace the e-safety policy.

Facebook has a facility where you can have 'friends'. This is designed to allow friends and family to access your personal information, post comments to you, read any posts/comments you make, look at your photographs, tag you (use your information on your behalf) and generally have easy access to all your information.

Privacy Settings

Unless you define your privacy settings carefully, Facebook shares all your information with everybody (defined as 'public' by Facebook). This would allow anybody to look at your posts, photographs etc. and re-post them elsewhere. This is how students are able to 'find' one another and if they so desire, members of staff.

To improve your privacy settings, please follow these steps.

From your homepage, click on the arrow in the top right of the screen and choose **privacy settings.**

Set your default privacy to friends.

This section is followed by five further categories.

1. **How You Connect**. Click edit settings and you will see five options. It is recommended that you set each option to friends (you may wish to choose a different option for **'Who can send you friend requests**, although friends of friends is the most secure). Click done.
2. **How Tags Work**. Click edit settings. It is recommended that you turn 'review' on (this means you have to agree to someone naming you in a photo etc). Choose friends for your **profile visibility**, for **tag suggestions** choose no-one. **Friends can check you into places** will be on, it is recommended that turn this off. Click done.
3. **Apps and Websites**. Click edit settings. Some apps need your data to locate you. It is recommended that you turn these off although this may affect functionality of some apps. Click back to privacy (top left).

4. **Limit the audience for past posts**. Click 'manage past post visibility'. Click limit old posts (this ensures only friends can see all historical activity). Click confirm. Click close.
5. **Blocked people and apps**. This enables you to choose to block certain individuals or apps/websites from using your page.

Profile Settings

1. Click on your name then Edit Profile.
2. There are options to change who can view your profile.
3. Click on 'view as' and the option on how your profile is viewed by the public .

Photographs

1. In your photo albums click on edit albums and change the privacy settings.

Once you have completed these steps, click on your name and you will return to the news feed.
This guide should be read in conjunction with Deyes e-safety and web 2.0 policy.