Fyling Hall School
E-Safety Policy

Fyling Hall recognises the internet and other digital technologies provide a vast opportunity for children and young people to learn. Unlike any other mode of technology, the internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop and enhance the curriculum to make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.

At Fyling Hall School we understand the responsibility to educate our pupils 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.

Fyling Hall has a zero tolerance policy towards cyber bullying and any incidents will be dealt with in line with the procedures laid out in the anti-bullying policy. The school views cyber bullying as the misuse of the digital technologies or communications to bully a person or group. Fyling Hall classes the following behaviour as cyber bullying:

- Abusive comments, rumours, gossip and threats made over the internet or using other digital communications. This includes internet trolling.
- Sharing pictures, videos or personal information without the consent of the owner and with the intent to cause harm or humiliation.
- Hacking into someone's email, phone or online profiles to extract and share personal information, or to send abusive or inappropriate content while posing as that person.
- Creating specific websites or groups that negatively target an individual or group, typically by posting content that intends to humiliate, ostracise or threaten
- Blackmail or pressurising someone to do something online they do not want to such as sending sexually explicit images.

This policy works in conjunction with other key policies (The Behaviour, Anti-Bullying and Safeguarding Policies) to safeguard the health and wellbeing of all our children.

This policy applies to all members of Fyling Hall School (including Trustees, staff, students, volunteers, parents/carers, visitors) who have access to and are users of Fyling Hall ICT equipment and the internet network.

Fyling Hall School
E-Safety Policy

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

Access to School Network

A domain username and password will be issued by the Head of ICT when the 'Acceptable Use Agreement' has been signed. A temporary password will be issued which should be changed the first time someone logs on to the network.

User profiles are issued depending on the required level of clearance appropriate to the individual. The varying profiles (Visitor, Pupil, Teacher & Executive) restrict access to the appropriate areas of the network.

Temporary access to the network is supplied to invited guests of the school through a visitor profile. This profile offers restricted access to the school network and the password is reset after each visitor has finished.

All users must keep their domain usernames ~~,~~and passwords secret. Staff should encourage pupils to keep their password secret to reduce the likelihood of pupils logging on as each other. Any device that can be used to access personal data must be locked or logged off when left unattended (even for very short periods).

Users must not allow others to use their account except for the purposes of teaching or support. Where a pupil uses an interactive screen or a computer whilst the teacher is logged on, data protection remains the teacher's personal responsibility.

Personal data is stored on the school's computer network, and can be accessed by staff (who have the appropriate permissions) in school. Any security breach must be immediately reported to the Head of ICT or the Headmaster; they will be treated seriously and could become a child protection issue.

Fyling Hall School
E-Safety Policy

Whole School Responsibility for E-Safety:

Within Fyling Hall all members of staff and students are responsible for e-safety, responsibilities for each group include:

Trustees

Trustees are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Trustee. The role of the E-Safety Trustee will include:

- regular meetings with the Head of ICT or Designated Senior Lead
- regular monitoring of e-safety incident logs
- regular monitoring of logs for key word and top 20 website searches
- reporting to relevant Trustees

Students

- Participating in and gaining an understanding of e-safety issues through the curriculum and enrichment activities.
- Compliance with the student's 'Acceptable Use Agreement' which students must agree to each time they use school ICT equipment either in the school or when remotely connected to the wireless internet.
- Reporting any e-safety issue to a teacher, member of staff or parent.
- Take responsibility for their own actions when using the internet and communications technologies.

All Staff

- Have a clear understanding of e-safety issues and the required actions if they have any concerns.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- Report any e-safety issues to the Head of ICT or the DSL as soon as the issue is detected.
- Comply with the staff Acceptable Use Policy (AUP) which staff must agree to each time they use the school ICT equipment either in the school or when remotely connected to the wireless internet.

Teaching Staff

- Educating students on e-safety when using the computers and re-enforcing this in the day to day use of ICT in the classroom.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit during their lessons.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Role & Responsibility of Key Staff in e-safety:

Trustees

- Approve and review the effectiveness of the E-Safety Policy and acceptable usage agreement
- The E-Safety Trustee should work with the E-Safety Co-ordinator to carry out regular monitoring of e-safety incident logs and monitoring logs and report to Governors at Full Governing Body meetings

Headmaster

- The Headmaster has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Head of ICT & Designated Senior Lead.
- The Headmaster and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headmaster is responsible for ensuring that the E-Safety Coordinator/Designated Senior Person and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headmaster/DSL will ensure that they support and guide those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also advise to those colleagues who take on important monitoring roles.

Network manager

- Ensure that the best technological solutions are in place to ensure e-safety as well as possible whilst still enabling students to use the internet effectively in their learning.
- users can only access data to which they should have right of access
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e-safety breach.

- Checks and audits all systems to ensure that no inappropriate data is stored or is accessible.
- Make sure no user is able to access another's files without permission
- Works with the Head of ICT and DSL to create, review and advise on e-safety and acceptable use policies.

Head of ICT

- Leads the development of the e-safety education programme for students and staff.
- Manages a parental awareness programme for e-safety.
- Deals with e-safety breaches from reporting through to resolution in conjunction with Network manager.
- Starts a written record of any e-safety breaches and collates any evidence
- Informs DSP of any e-safety issues, evidence, action taken and if further action is required.
- Works with the Network manager to create, review and advise on e-safety and acceptable use policies.

DSL (e-safety manager)

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- liaises with the Local Authority/relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Trustee to discuss current issues, review incident logs and filtering/change control logs
- reports regularly to the Headmaster on any e-safety issues.

Parents& Carers

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- School Policy available on the School Website
- E-Safety booklet available on website
- All parents read and sign 'Acceptable Use Agreement' for their child
- Letters, newsletters, and updates on web site
- Parents/Carers evenings/sessions
- High profile events/campaigns eg Safer Internet Day

How to report a Problem or Concern

Staff

As with all safeguarding staff are encouraged to seek advice from Head of ICT, DSL or Headmaster if they have any issues or concerns related to any aspect of e-safety.

If a member of staff has a specific concern regarding a pupil or a member of staff they should complete the 'e-safety concern form' which is located in the e-safety folder in the Teachers drive. When completing this form staff need to provide as much information and supporting evidence as they can. When this form has been completed it should be returned to either the Head of ICT or if it is viewed as a Safeguarding issue straight to the DSL.

This will result in an investigation into the issue/concern and a time line of events being started by the Head of ICT. If the issue/concern is deemed to be a safeguarding issue then the DSL will lead the investigation and oversee it to a conclusion. At this point if deemed necessary the appropriate outside agencies will be contacted for advice on how to proceed (police & social care) and the school will act on the advice given.

When disciplinary action is required as a result of an investigation the following process will be used. If the outcome is a minor infringement (level 1 or 2) then an appropriate punishment will be issued and recorded by the Head of ICT. A more serious infringement (Level 3 or 4) will be referred to the Headmaster for a decision about sanctions which will be recorded in the central punishment register. Parents will be contacted about the outcome of an investigation if a sanction is required.

Pupils

Pupils should report any concerns they have regarding e-safety and also seek advice and guidance when they are unsure about any e-safety issues.

Pupils should contact the Head of ICT to report a concern. However pupils may also speak to any other member of staff if they do not wish, or are unable to speak to the Head of ICT.

If pupils prefer to write their concerns down they can post their comments in the secure reporting box found in the ICT room.

Pupils may also email the Head of ICT or the Headmaster.

Pupils are made aware of the e-safety folder on their computer desktop and this contains details on how they can report a problem/issue.

Parents/guardians

Fyling Hall School
E-Safety Policy

Parents and guardians are welcome to contact the school for advice about any e-safety issues, concerns or questions. If a parent has a specific concern or complaint about e-safety they would like to be investigated they should contact the relevant staff member from the list below. You can contact then on the school number or by email.

Wendy Banks	Head of ICT	w.banks@fylinghall.org
Adele Gilmour	Safeguarding DSL	a.gilmour@fylinghall.org
Steven Allen	Headmaster	headmaster@fylinghall.org

How we ensure e-safety in the classroom:

Educating students in e-safety

A clear objective of Fyling Hall is to educate students in safe use of ICT and the internet. We feel this is one of the best ways to minimise the potential for any e-safety issues to occur.

Students will receive specific e-safety lessons aimed at ensuring that:

- Students know the e-safety risks that exists and how to identify when they are at risk.
- Students know how to mitigate against e-safety risks by using e-safe practices whilst online.
- Students aware of the e-safety folder on their desk–top and guided through how to use the information and support contained in the folder.
- Students know when, how and to whom to report instances when their e-safety may have been compromised.
- Students know that they are in an environment that encourages them to report e-safety issues without risk of reprimand, humiliation or embarrassment.

The school will utilise the Think U Know programme by the governments Child Exploitation and Online Protection (CEOP) centre as one of the primary education tools.

In addition to the specific e-safety content of the ICT curriculum all members of staff will have a duty to reinforce e-safety practices wherever possible. They will offer students advice and support in the classroom where minor e-safety incidents have occurred.

E-Safety education information will have high visibility in all areas of the school.

Educating Staff in e-safety

Induction: As part of the induction process all new staff will have to read and sign the 'Acceptable Use Agreement' to be issued a domain username and password. The Head of ICT will go through the agreement, the e-safety policy and identify the role staff play in e-safety with the new staff and answer any questions they might have.

Staff will be made aware of the e-safety folder on the school desktop which is for both pupil and staff to use as a source of reference, support and advice.

Inset: As part of the ongoing professional development of staff, sessions will be organised to identify new e-safety issues, discuss e-safety and the application of this policy in the school.

How e-safety is monitored

- The ICT department will monitor the students ICT activity using a key word search once a month which will flag students or websites with potential e-safety issues.
- The ICT department will once a month review the Top 20 accessed websites on the network to track any websites which could potentially present an e-safety issue.
- Mobile devices are prone to the same checks while using the school wireless network.
- The E-Safety manager will periodically review the E-Safety log to track and trends and use the information to look at ways of improving the student's e-safety.
- Teaching staff will directly monitor the students ICT and internet use in the classroom.

Filtering software (Smoothwall) restricts pupils and staff with what websites they can access using a school account. Neither staff nor pupils can install any software onto the school network. The network is regularly checked for any unsuitable filetypes (such as .exe files) and sanctions imposed if any are found.

Smoothwall is also a comprehensive firewall, protecting the school network from outside attack.

Acceptable Use for Staff

All staff must sign 'The Fyling Hall Code of Conduct' and 'The Acceptable Use Agreement'. Staff must adhere to the expectations and guidance about communication with pupils. Any communication should be conducted through school platforms only.

Communication:

Fyling Hall School
E-Safety Policy

Communication between students and staff, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites, social networking sites, online gaming and blogs.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the Headmaster/DSL – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, chat, VLE etc) must be professional in tone and content.

Social Media:

Staff should only use social networking sites for personal use. The school strongly advises that profile and photos of the member of staff are 'locked down' as private so that students or parents do not have access to your personal data or images. The school strongly advises Staff deny current or recent students access to your profile. Staff should always consider their professional identity when using social media and avoid activity which could damage either their own or the schools reputation.

School staff should ensure that:

- Personal social networking and media systems should only be used in a positive fashion when referencing the school. Staff should understand that bringing their profession and/or the school into disrepute will result in disciplinary proceedings.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Staff members should never harass, cyberbully, discriminate on the grounds of sex, race or disability or defame a third party when posting on these public forums
- Staff should never express or support extreme religious or political views on these public forums.
- Personal opinions should not be attributed to the school or the governing body.

Failure to follow these guidelines could result in disciplinary action.

Fyling Hall School
E-Safety Policy

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- E-safety induction for new staff
- Risk assessment, including legal risk.

Use of Pupil Images

All new parents must complete a 'Consent Form to use images and photographs' prior to starting Fyling Hall. This form must be completed and returned by parents giving a clear indication if consent is not given. A record of students where consent has not been given will be recorded and made available for staff to view on the Safeguarding noticeboard in the Staffroom. Images, photographs and videos of Fyling Hall Students can only be used in accordance with the agreement and any intentional misuse may result in the School disciplinary procedure being implemented.

Bring Your Own Device (BYOD):

As a rural boarding school Fyling Hall allows students to bring mobile devices to school for safety and communication with home.

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.

- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Students receive training and guidance on the use of personal devices.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss, theft, change of ownership of the device will be reported.

Misuse & Sanctions

How the School will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headmaster.

Students:

Level 1 infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

Level 1 Sanctions

- Removal of mobile phone (or other new technology) until the end of the day
- Removal of Internet access rights for 24 hours
- Contact with parents

Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Accidentally accessing offensive material and not notifying a member of staff of it

Level 2 Sanctions

- Removal of mobile phone (or other new technology) for 3 school days (in the case of daily pupils any devices brought into school must be handed in at the start of the school day and collected at the end of the day)
- Contact with parents
- Removal of Internet access rights for 3 days
- Referral to e-safety Manager for future monitoring purposes

Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Transmission of commercial or advertising material

Level 3 Sanctions

- Removal of mobile phone (or other new technology) for 1 week (7 days) (in the case of daily pupils any devices brought into school must be handed in at the start of the school day and collected at the end of each day)
- Contact with parents
- Removal of Internet access rights for 1 week (7 days)
- Referral to Head of ICT for monitoring purposes and re-education

Level 4 infringements

- Continued sending of emails or instant messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised ~~1988~~ 2018
- Bringing the school name into disrepute

Level 4 Sanctions

- Indefinite removal of mobile phone (or other new technology) (in the case of daily pupils, any devices brought into school must be handed in at the start of the school day and collected at the end of each day)
- Contact with parents
- Indefinite Removal of Internet access rights
- Indefinite Removal of Computer access rights to any part of the school network and school computer equipment
- Referral to e-safety Manager and Headmaster
- Possible suspension / exclusion at the discretion of the Headmaster
- Referral to police if appropriate
- Referral to Local Authority e-safety officer if appropriate

Staff & Trustees:

Level 1 infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.

- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or licence e.g. installing unlicensed software on network

Level 1 Sanctions

- Referral to Head of Department / e-safety Manager / Headmaster
- Warning given in line with School disciplinary procedures

Level 2 infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised ~~1988~~2018;
- Bringing the school into disrepute.

Level 2 Sanctions

- Referral to Headmaster and follow School disciplinary procedures
- Referral to Trustees
- Referral to Police & relevant outside agencies if required

Child Pornography:

In the case of child pornography being found, the member of staff will be immediately suspended and the School disciplinary procedures implemented.

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Where appropriate, involve external agencies as part of these investigations.
-

How will staff and students be informed of these procedures?

- Procedures are included within the school's e-safety / Acceptable Use Policy. All staff are required to sign the school's e-safety Policy acceptance form;
- Pupils will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'. Pupils are required to sign an age appropriate e-safety / acceptable use form;

- The school's e-safety policy will be made available to parents who are required to sign an acceptance form when their child starts at the school.
- Staff are issued with the 'What to do if?' guide on e-safety issues.

Useful websites and contacts:

www.childnet.com
www.saferinternet.org.uk
www.nspcc.co.uk
www.internetmatters.org
www.childline.org.uk
www.cybersmile.org

- UK Council for Child Internet Safety (UKCCIS)
- NAACE
- EU Kids Online
- Child Exploitation Online Protection Centre (CEOP)

Updated: March 2019 by S.Allen & R.Mansoor To be reviewed by January 2020