FRED LONGWORTH HIGH SCHOOL

Electronic safety policy

This Policy was approved by:

Full Governing Body: 23 November 2020

Date for Review: November 2021

1. Rationale

At Fred Longworth High school, we acknowledge that digital technologies are integral to the lives of young people both within and outside of school. The Internet and other technologies are powerful tools which open up new opportunities. All young people have an entitlement to access such technologies, to enhance motivation and engagement and thus facilitate continued improvements in standards across all curriculum areas. The requirement to ensure that young people are able to use technologies appropriately and safely should be addressed as part of the wider duty of care to which all those who work in schools are bound. This E-Safety policy should ensure safe and appropriate use of technology. The implementation of this strategy involves all stakeholders in the school community.

"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool, we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim."

Dr Tanya Byron; "Safer children in a digital world": The report of the Byron Review.

At Fred Longworth High School, we equip students with the skills and knowledge they need to use technology safely and responsibly, and manage the risks, wherever and whenever they go online; promoting safe and responsible behaviours in using technology at school, in the home and beyond.

2. Purpose

This policy addresses the potential risks associated with digital technology including but not exclusively:

- access to illegal, harmful or inappropriate images, harmful websites and unsuitable video/internet games.
- the risk of being subject to grooming via the internet, and possibly meeting high risk individuals in person.
- the sharing and/or distribution of personal images without the individual's consent or knowledge.
- inappropriate communication with others including strangers.
- cyber bullying.
- illegal downloading of files.
- the inability to evaluate the accuracy and relevance of information on the internet.
- plagiarism and copyright infringement and unauthorised access to, or loss of, or inappropriate sharing of personal information.
- the risk of becoming involved in extremist groups or 'radicalised' (Prevent Duty).

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying
- Cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

4. Roles and responsibilities

4.1 The governing body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Anita Mullineaux.

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see ICT policy and Handbook)

4.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The designated safeguarding lead

Details of the school's DSL are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Updating and delivering staff training on online safety (appendix 1 contains a self-audit for staff on online safety training needs)
- Ensuring that any online safety incidents are logged (appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body

4.4 The ICT manager

The ICT manager is responsible for:

- The NetSupport System, is used to alert staff to inappropriate content. This has filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. In such cases Mrs Calcutt is alerted and deals with this through the appropriate member of staff.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- The system is monitored 24/7 by a combination of security systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and cyber bullying policy
- If staff or students discover an unsuitable site, this must be reported to IT Systems Support Staff and the relevant Head of Year.

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. Classroom teachers should be vigilant for the misuse of IT within their lessons. If a student is found to be misusing the Internet this will be treated very seriously and may result in a student being banned from using IT within the school for a fixed period of time. Other sanctions will follow if this persists.

4.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see ICT policy and handbook), and ensuring that students follow the school's terms on acceptable use (see ICT policy and handbook)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

4.6 Parents

Parents are expected to:

- Notify the headteacher, pastoral deputy head or Head of Year of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see ICT policy and handbook)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - UK Safer Internet Centre

Hot topics - Childnet International

Parent factsheet - Childnet International

4.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (see ICT policy and handbook).

5. Educating students about online safety

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

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they 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 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

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

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy is accessible to parents and carers. E-Safety information for parents is published on the school website.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

The school maintains a current record of all staff and students who are granted access to school ICT systems.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Parents and carers will be asked to support Fred Longworth's ICT Guidelines by signing the relevant consent form (see ICT Policy and handbook)

More information is set out in the acceptable use agreements in the ICT policy and handbook.

The school Internet access is designed expressly for student use and will include filtering appropriate to the age of students.

- Clear boundaries are set for the appropriate use of the Internet and digital communications and discussed with staff and students.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- We ensure that the use of Internet derived materials by staff and by students complies with Copyright Law.
- During PSHE Day, activities reinforce the message of safe Internet use to Year 7.

Assemblies are held with all year groups to teach students about e-safety related matters, positive contribution and potential dangers of using the Internet.

8. The use of e-mails

Electronic messaging includes, but is not limited to, e-mail, SMS/MMS messages, Instant messaging, messaging and chat within apps, video and audio conferencing and any future developments of those technologies.

- Students may only use approved messaging accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mails.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

9. Social networking and personal publishing

We control access to social networking sites. Through assemblies and pastoral lessons all students receive age appropriate training on keeping safe on the Internet. This uses materials from CEOP. Assemblies are taken by senior staff. During this time, students are advised:

1. Never to give out personal details of any kind that may identify them, their friends or their location.

2. Not to place personal photos on any social network space without considering how the photo could be used now or in the future.

3. To set passwords, to deny access to unknown individuals and to block unwanted communications.

4. Who to see in school if they feel unsafe on the internet and how to use the ThinkuKnow website to report abuse.

5. That they should only invite known friends and deny access to others.

- In addition to this all Year 7 students receive training in ICT on E-Safety.
- Internet safety posters are displayed in all rooms where computers are used.
- E-Safety advice for students and parents is published on the school website.
- This e-safety information for students and parents on the school website is detailed and updated regularly. Important bulletins are regularly sent out via the school's official Twitter and Facebook account.
- Students are informed that network and Internet use is monitored.
- Students are taught about E-Safety annually during the weekly assemblies and PSHE days. Assemblies are followed up in pastoral time.
- The School Council is consulted on E-Safety issues.

10. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are not to be used in school.
- Sending abusive or inappropriate text messages, filming or taking photographs on personal devices in school is not allowed and is dealt with following the school discipline policy.
- Staff are advised to use a school phone where contact with students is required. The school has mobile phones for use during school trips.

11. Protecting personal data

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018 and the GDPR.

12. Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by the appropriate Head of Year or, if necessary, a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher /Pastoral Deputy Head.

- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.

13. Staff and the e-Safety policy and work devices

- All staff have access to the School E-Safety Policy and its importance will be explained.
- Staff are informed that network and Internet traffic is monitored and can be traced to the individual user.
- Staff that manage filtering systems or monitor ICT use are supervised by Senior Management and work to clear procedures for reporting issues.
- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in the ICT policy and handbook.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
- Staff are advised always to maintain a professional relationship particularly on Social Networking Sites such as Facebook or Twitter.
- Fred Longworth High School maintains a Facebook and Twitter account for the purpose of engaging parents and the local community in school projects and activities. This is closely supervised by a senior member of staff.
- Staff are kept up to date through CPD with potential issues surrounding E-Safety.
- Advice to staff can be found in the 'Staff Code of Conduct'.
- If staff have any concerns over the security of their device, they must seek advice from the ICT manager.
- Work devices must be used solely for work activities.

14. Training of staff

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

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

15. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

16. Blended Learning

Due to the Covid 19 pandemic we have introduced blended learning into the curriculum. Staff have received training on the platform of Microsoft TEAMS and have been trained in the safety of delivering online lessons. Staff have a protocol slide which is delivered at the beginning of each lesson (Appendix 3)

Children have also received training and how to access online learning and students continue to develop their skills through blended learning training each week in registration.

Expectations are the same as a classroom lesson and if students do not meet expectations the behaviour policy is followed.

17. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 2.

The school's lead staff for this policy are the Director of Inclusion and the Pastoral Deputy Head. This policy will be reviewed every year. At every review, the policy will be shared with the governing body.

18. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Cyber –Bullying policy

Mobile phone policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

ICT and internet acceptable use policy

Staff Code of Conduct

Appendix 1: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 2: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 3: TEAMS Protocols for blended learning