FRED LONGWORTH
HIGH SCHOOL

Online Safety Policy

January 2024

This Policy was approved by:

The Board of Trustees: January 2024

Date for Review: January 2026

Policy Statement Online Safety

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 Online 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.

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).

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

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

Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Online Safety Act October 2023

It also refers to the DfE'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.

Roles and responsibilities

The Board of Trustees

The Board of Trustees have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Board of Trustees must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The trustees will review the DfE filtering and monitoring standards, and discuss with the DSL what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The trustee who oversees online safety is Carole Gradwell.

All trustees will:

- Ensure they have read and understand this policy
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

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

The Designated Safeguarding Lead (DSL)

Details of the school's DSL Mr Whalley and Deputy DSL Mrs Waring are set out in our child protection and safeguarding policy as well as 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy – this is done through CPOMS
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

The ICT manager

The ICT manager **Mr O'Neill** is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- The Net Support system is used to alert staff to inappropriate content. In such cases Mrs V. Barnes (IE Manager) is alerted and deals with this through the appropriate member of staff. Any worrying content is flagged and the relevant HoY/DSLs are alerted through a CPOMS referral. Any urgent concerns are passed on verbally as soon as possible.
- Conducting a full security check and monitoring the school's ICT systems on a daily basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Assisting Heads of Year/DSLs with students who breach the ICT acceptable use policy.

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, and ensuring that students follow the school's terms on acceptable use.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting to Mr Whalley.
- Staff are informed that network and Internet traffic is monitored and can be traced to the individual user.
- Following the correct procedures as set by the ICT Manager if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged 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.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.
- If staff or students discover an unsuitable site, it must be reported to IT Systems Support Staff and the relevant Head of Year/DSLs
- We 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.
- Classroom teachers should be vigilant for the misuse of IT within their lessons.
- 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 X (formerlyTwitter) 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 Online safety.
- Advice to staff can be found in the 'Staff Code of Conduct'.

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.

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher 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.

Parents/carers 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 resource sheet – Childnet International

Educating students about online safety

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

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships and sex education and health education in secondary schools

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
- 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**, students will know:

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

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

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

Educating parents about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website and during our Online Safety Evening. This policy will also be shared with parents/carers.

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

Cyber-bullying

Definition

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

Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their tutor groups, in line with the Personal Development (PD) Curriculum.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes within PD lessons, and other subjects where appropriate.

The school also shares information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining electronic devices

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

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

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

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

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

- Report it to the police*

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

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

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

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

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Fred Longworth High School recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Fred Longworth High School will treat any use of AI to bully students in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Fred Longworth High School.

Acceptable use of the internet in school

All students, parents, staff and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

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.

Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them during their time on premises unless given permission from a member of staff.

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

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager.

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. 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 disciplinary procedures. 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.

Training

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 at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example, through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

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.

Volunteers will receive appropriate training and updates, if applicable.

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

The use of e-mails

- Students may only use approved e-mail accounts on the school system. These include emails using Office 365 and Satchel.
- 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.

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. 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 Online safety.
- Internet safety posters are displayed in all rooms where computers are used.
- Online safety advice for students and parents is published on the school website.
- This Online 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 Online safety annually during the weekly assemblies and PSHE days. Assemblies are followed up in pastoral time.
- The School Council is consulted on Online safety issues.

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.

Authorising Internet access

- When logging on to the school system, both students and staff agree to the Acceptable Use Policy.
- The school maintains a current record of all staff and students who are granted access to school ICT systems.
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Parents/carers will be asked to support Fred Longworth High School's ICT Guidelines by signing the relevant consent form.

Protecting personal data

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

Handling Online 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 Head teacher/Pastoral Deputy Head.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every two years by the Senior Deputy Head Mr Whalley. At every review, the policy will be shared with the Board of Trustees.

The school's lead staff for this policy are the Director of Inclusion and the Pastoral Deputy Head.
This policy should be read in conjunction with the school's Behaviour Management Policy, Anti-Bullying Policy, Cyber-Bullying Policy and Mobile Phone Policy.