Chigwell School

Mr D.A.P. King
Head

dking@chigwell-school.org
D: +44 (0)20 8501 5701
T: +44 (0)20 8501 5700
High Road, Chigwell, Essex IG7 6QF
www.chigwell-school.org

Staff champion	AFS
Last Reviewed by Governors	October 2025
Next Review by Governors	October 2027
Committee	Risk, Wellbeing and Compliance

E Safety Policy

1. Introduction to E Safety Policy 2
2. Roles and Responsibilities 2
3. Teaching and Learning 3
4. Managing Information and Systems 4
5. Response to Incidents of Concern 5
6. Anti-Cyberbullying 5
7. Prevent: The Issue of Radicalisation 6
8. Use of Personal Cameras, Mobile Phone or other Recording Devices 7
9. Training for Pupils Parents and Staff 7
10. Use of School Wifi on Personal Devices 7

Appendix A Biometric Information 9
Appendix B Pupils' Use of ICT Agreement 11

1. Introduction

This policy applies to all members of the Chigwell School community (including staff, pupils, Governors, volunteers and visitors) who have access to and are users of the School ICT systems, both in and out of school.

The School fully appreciates the fundamental relationship between E Safety and Pupil Safeguarding and its legal obligations to safeguard all of its pupils (See *'Safeguarding and Promoting Children's Welfare' Policy and 'Keeping Children Safe in Education', DfE, September 2025*) The School recognises that the *Education and Inspections Act 2006* empowers Headteachers to carry out reasonable regulation of the behaviour of pupils when they are away from the school site. This is especially pertinent to incidents of cyberbullying, or other E-Safety incidents, which may occur away from the School premises, but are linked to membership of the School. The *2011 Education Act* gave greater powers to Headteachers with regard to searching of electronic devices and the deletion of school data. The School also understands its legal responsibilities under the Prevent Duty Guidance for England and Wales July 2015, to take every effort to prevent individuals from being drawn into terrorism through the internet or by other means, and to challenge extremist ideas propagated by terrorist organisations.

The School will deal with E-Safety incidents with regard to this policy and other relevant policies (*Anti-bullying Policy, Behaviour and Sanctions Policy and Safeguarding and Promoting Children's Welfare*) and seek to keep parents fully informed of any E-Safety incidents or threats.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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 scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

commerce: the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

2. Roles and Responsibilities

Board of Governors:

The Board of Governors is responsible for the approval of the E-Safety Policy and for reviewing the effective implementation. The Safeguarding Governor carries out reviews of filtering and monitoring and will review the DfE guidance on Generative AI: product safety expectations with IT staff.

Head:
The Head has a duty of care for ensuring the safety (including E-Safety) of all members of the school community.

Deputy Head (Staff & Systems):

- Takes responsibility for E-Safety issues and has a leading role in establishing and reviewing the E –Safety Policies and documents
- Runs regular network security 'health checks' with the network manager including monitoring of filtering system
- Liaises with technical staff to ensure network security
- Liaises with the Designated Safeguarding Lead to review reports of E-Safety incidents
- Reports regularly to SMT regarding E-Safety issues
- Reviews any suspicious search findings through weekly report
- Coordinates delivery of E-Safety through curriculum, Wellbeing (PSHE), assemblies and drop-down days

IT Manager is responsible for ensuring:

- That the School's technical infrastructure is secure on a day-to-day basis
- That users may only access the networks and devices through a properly enforced password protection policy
- That age-appropriate filtering and monitoring systems are applied for all pupils
- That they keep up to date with e-safety technical information and brief key staff accordingly
- That the use of the network is monitored regularly in order that any misuse or attempted misuse can be reported to the Deputy Head (S&S).
- That monitoring software of systems are implemented and updated
- That actions following concerns or checks to systems are completed

Designated Safeguarding Lead and Deputies:

The DSL has lead responsibility for safeguarding and online safety. This includes:

- understanding the filtering and monitoring systems and processes in place
- Understanding E-Safety issues and aware of the potential for serious child protection/safeguarding issues arising from the use of technology in and out of school
- Providing training and advice for staff, pupils, parents and Governors
- Being made aware immediately of any child protection/safeguarding issues relating to the use of technology e.g. sharing of personal data, sexting, grooming, illegal materials, cyberbullying etc.
- Managing filtering and monitoring reports
- Checking filtering and monitoring system are working
- Liaising with the Deputy Head (S&S) on all reported E-Safety incidents

Teaching and Support Staff are responsible for ensuring that:

- They have read the E-Safety Policy
- They report any suspected misuse or problems to the Deputy Head (S&S)
- Digital communications with all members of the Chigwell School community (pupils, parents, colleagues) must always be conducted on a professional level and only carried out using official school systems

- They monitor the use of digital technologies (mobile devices, camera etc.) in lessons and other school activities and implement current policies with regard to these devices
- Internet use in lessons is pre planned and closely monitored to ensure pupils do not gain access to inappropriate material (e.g. pornography or websites depicting violence or promoting extremist political views)
- Any suspicion of child abuse or any incident which may be considered a child protection/safeguarding issue should immediately be reported to the Designated Safeguarding Lead or one of her deputies.
- If teaching content which could cause a spike in logs (for example drug education) that this is reported
- Any unreasonable restrictions to teaching and learning materials are reported
- Any misspelling or abbreviations that allows access to unacceptable content in reported

Carry out professional development reviews and regular supervision meetings
Pupils:

- Are responsible for using the School's ICT systems, in school or remotely, in accordance with the *Pupils Use of ICT Agreement*
- Must report any instance of abuse, misuse or access to inappropriate materials to a member of staff
- Must know and understand policies on the use of mobile phones and digital cameras. They should also know and understand policies on the taking/use of images and on cyberbullying
- Must understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of School, if related to their membership of the School.

Parents:
Parents play an important role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' E-Safety evenings, SchoolPost, letters and other means. Parents may be encouraged to support the School in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events (do not post on social media)
- Their child's personal devices in the School (see Pupils Use of ICT Agreement)

Please see the Child Protection and Safeguarding Policy for full details.

3. Teaching and Learning

Internet use is an integral part of the curriculum and is a necessary tool for learning. The School has a duty to provide pupils with good quality internet access as part of their learning experience and recognises a duty to teach pupils how to evaluate internet information and to take care of, and responsibility for, their own safety and security.

Internet access is available to all staff and pupils through their school username and password. The School reserves the right to withdraw access to the internet and other ICT systems if it has concerns about the way it is being used by any individual. Pupils will be taught what internet use is acceptable and what is not, and will be given clear objectives for internet use.

Internet use in lessons is pre planned and closely monitored to ensure pupils do not gain access to inappropriate material (possibly pornography or websites depicting violence or promoting extremist political views).

Pre Prep pupils using the computer suite, laptops or tablets must be supervised by an adult at all times and any software, games or apps used must be from a pre-approved selection checked and agreed by the Head of Pre Prep and ICT Coordinator.

Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

Senior School pupils who are using a school tablet, or their own device, can only do so if they have completed the Pupil Use of ICT Agreement.

All devices will automatically connect to the School Wi-Fi when they enter the premises. This will encourage pupils to use the filtering system and not 4G/5G.

Pupils below Year 9 are not permitted to use their own phones/devices during the school day.

Remote Learning
If it is necessary to return to remote learning, pupils and teachers will be reminded of the expectations the School has of them when learning online. The Covid-19 Remote Learning plan will be updated and distributed to all stakeholders.

Gateway:

- Access to the School's Gateway VLE is obtained via the school website
- Access to Gateway is password protected
- Only staff have the necessary permissions to upload material onto Gateway
-

4. Managing Information and Systems

- The security of the School information systems and users will be reviewed regularly by the Deputy Head (Staff &Systems) and the IT Manager
- Virus protection will be updated regularly
- Personal data sent over the internet or taken off site will be encrypted
- The use of user log-ins to access the School's network systems will be enforced
- Multi-factor authentication will be enforced for access to school resources outside the school network

Broadband Filtering and Monitoring:
The School will take reasonable precautions to ensure that users access only appropriate material. However, owing to the nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer, or device linked to the school Wi-Fi. The School cannot accept liability for the material accessed or any consequences resulting from internet use. Methods to identify, assess and minimise risks, will be reviewed regularly by the Deputy Head (S&S) and the IT Manager.

The School's broadband access will include filtering appropriate to the age and maturity of pupils. Breaches of filtering will be reported to the Deputy Head (S&S) or the IT Manager. Offenders may be blocked from the network for a fixed period, or, if the breach is such as to constitute a breach of the law, the incident will be reported to the appropriate agencies such as the Police or CEOP.

The School will use the DFE's 'plan technology for your school service' to self-assess against the filtering and monitoring standards.
The school has consulted the following when considering filtering and monitoring across the school:

- UK Safer Internet Centre: https://saferinternet.org.uk/guide-andresource/teachers-and-school-staff/appropriate-filtering-and-monitoring.
- South West Grid for Learning (swgfl.org.uk)
- DfE Generative AI: product safety expectations to support schools to use generative artificial intelligence safely

If staff or pupils discover unsuitable sites, the URL will be reported to the Deputy Head (S&S) who will deal with the concern as appropriate.
Guidance taken from *UK Safer Internet Centre: appropriate filtering and monitoring* and *National Education Network.*

Virtual Private Networks (VPNs):
The use of Virtual Private Networks (VPNs), proxy servers, or any other technology designed to bypass the School's filtering and monitoring systems is strictly prohibited on all devices connected to the School network

VPNs and similar tools circumvent the safeguarding measures put in place to protect pupils and undermine the School's ability to monitor online activity for child protection purpose.

Use of VPNs or proxy services will be treated as a serious breach of this policy and may result in loss of network access and disciplinary action in accordance with the School's Behaviour and Sanctions Policy

Any pupil found using such technology must report this immediately to the Deputy Head (S&S) or a member of teaching staff

Emerging Technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the Pupil's Use of ICT Agreement. Pupils are encouraged to connect all devices to the Wi-Fi (as opposed to 3G/4G/5G) at home and at School to ensure that appropriate filters are in place.

Biometric Data
Biometric information is information about a person's physical or behavioural characteristics that can identify them. Chigwell School is using Biometric finger patterns for Senior School pupils for tablet storage lockers. The School has followed the New Government Legislation, The Protection of Freedoms Act 2012 to ensure that we have the correct parent, guardian and pupil permission to store this data. Please see Chigwell School Biometric Information and Consent form for the Use of Biometric Information (Appendix A) for further details.

Network Passwords
Network passwords will be changed at least twice per year and must be at least 10 characters long and alpha numeric (i.e. contain letters and numbers).

Visitors
Visitors will be granted access to the School Wi-Fi. This is available on request from Reception. They will have access to the internet (this will be filtered) for a limited period of time and a maximum of five days. They will not have access to any other part of the school network. Visitors requiring access for longer than five days, should ask their school contact or sponsor to request a Wi-Fi login from the IT helpdesk.

5. Response to Incidents of Concern

- All members of the school community will be informed about the procedures for reporting E-Safety concerns, such as breaches of filtering, cyberbullying, accessing illegal content.
- All members of the school community have a responsibility to report any concerns or breaches of procedure as soon as possible.
- All staff and pupils have access to the 'confide' button on the computers.
- Any issues or concerns must be reported immediately to the Deputy Head (S&S).
- Any concerns regarding safeguarding will be reported to the Designated Safeguarding Lead.
- The School will manage E-Safety incidents in accordance with the school disciplinary policies where appropriate.

6. Anti-Cyberbullying

Information Technology plays an important and generally positive role in the lives of those living in the 21st Century. Chigwell School is committed to helping all members of the school community to understand both the benefits and the risks so that children and young people are equipped to use the technology available to them safely and responsibly.

On the site http://www.cyberbullying.org/ it is stated that "*Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others*."

Cyberbullying is unacceptable and forms part of our Anti\Bullying Policy. However, several characteristics distinguish cyberbullying from other forms of bullying, including:

- Students who are victimised have no place to hide, and can be targeted at any time and in any place.
- Cyberbullying can involve a very wide audience (e.g. through the circulation of video clips on the Internet), although the bully may not be aware of the audience's reactions.
- Students who cyberbully others may consider that they are protected by the anonymity of electronic forms of contact.
- As with some indirect traditional bullying, students who cyberbully do not usually see the response of the victim, changing the satisfactions or inhibitions normally generated by bullying.

Please refer to the Anti Bullying Policy.

7. Prevent: The Issue of Radicalisation

Chigwell School recognises that The Counter-Terrorism and Security Act 2015, places legal responsibility on schools to take every effort to prevent individuals from being drawn into terrorism, and to challenge extremist ideas propagated by terrorist organisations.

We approach these issues in four ways:

- Providing a safe online environment
  The School has strong filters in place to block pupil access to violent or otherwise inappropriate materials. Pupils are required to electronically sign the Pupils' Use of ICT Agreement that specifically prohibits them from seeking to access such sites. The language used in these policies is age appropriate and must be electronically signed before pupils have access to the internet. Internet usage is monitored on a weekly basis and pastoral and/or disciplinary response may follow if a pupil's usage breaches our rules or raises concerns. The School will also seek to block specific sites and

search terms if they appear to pose a risk to our pupils. Furthermore, pupils receive advice and instruction from teaching and pastoral staff on safe internet usage.

- Assessment of Pupil Behaviour
  The pastoral monitoring systems of the School have a vital role to play in preventing radicalisation of pupils. At Chigwell pupils are monitored closely by Tutors and Housemasters/mistresses/HoY and issues of concern are discussed at pastoral meetings. Concern can be raised and logged by any teacher using the 'Concerns' tab on iSAMS. This will immediately email the pupil's tutor and Housemaster/mistress/HoY. Where necessary a pastoral intervention or even counselling may be provided. The School will also seek further advice when concerns regarding pupil radicalisation arise.

- Staff Training and information
  The School recognises that it has a responsibility to provide INSET to staff on the issue of radicalisation to ensure that they remain vigilant and informed on the issue. It will also ensure staff are aware of how to respond appropriately to concerns about the possible radicalisation of a pupil.

- Promoting Fundamental British Values
  The School will vigorously promote fundamental British values such as democracy, the rule of law, individual liberty, mutual respect for and tolerance of those with different faiths and beliefs, and for those without faith through its Wellbeing (PSHE) Programme, Chapels, Assemblies, the curriculum and all other daily interactions between pupils and staff.

The Government also provides contact details for alerting authorities to suspected terrorist activity. These include the DfE dedicated telephone helpline and mailbox for non-emergency advice for staff and Governors: 020 7340 7264 and in addition to the local Police on 101. In an emergency ring the Police on 999.

8. Use of Personal Cameras, Mobile Phone or other Recording Devices

We accept that on occasions in parts of the School, parents/carers may record sports day, outings, Christmas and fundraising events by video or taking photographs but always in full view of all attending. Parents/carers may only upload any images or videos of their own children onto any social media site.

- Early Years Foundation Stage
  Children's safety and welfare is paramount. All children in our Reception class have their photographs taken to provide evidence of their achievements for developmental records. Photographs may be taken during indoor and outdoor play and displayed in albums or a child's development records for children and parent/carers to look through. Staff, visitors, volunteers and students are not permitted to use their own cameras or mobile phones to take or record any images of children at any time. Staff should not use their personal device to record images of pupils, unless they are using the Photo Ghost App.

- Mobile Phone Use: Pupils
  Please refer to Pupil Mobile Phone Policy

- Mobile Phone Use: Staff
  Please refer to Staff Code of Conduct

9. Training for Pupils, Parents and Staff on How to Keep Children Safe

The School fully appreciates the fundamental relationship between E Safety and pupil safeguarding and its legal obligations to safeguard all of its pupils. The School has a robust network and age-appropriate filtering system that is regularly checked by the IT Manager and DH (S&S). Staff and pupils have received training relating to E Safety and they have been advised of what they should do if a problem occurs. All Chigwell computers have a 'Confide' button and pupils or staff can alert members of staff to any issue they or others may be facing.

The School encourages pupils to build resilience in order to protect themselves and their peers whilst online. Pupils should recognise it is their own responsibility to maintain a secure online profile. Students are shown the significance and the advantages of the internet, but also shown its dangers by being alerted to a safeguarding and anti-bullying strategy in order to keep them safe in the real and the virtual world. There are regular discussions of online safety, the personal limits that should be put in place in order to maintain privacy, and what to do if a pupil is victim to - or viewer of - any form of cyberbullying.

Further provision is delivered through the KS1, KS2 and KS3 ICT Computer Science curriculum and across departments; the Wellbeing (PSHE) programme; assemblies, and external speakers.

Staff and parents also receive annual training and regular updates regarding keeping safe online. Advice is given regarding personal safety online e.g. phishing, ransomware etc. Staff and parents also receive advice regarding keeping the pupils safe online.

http://www.childnet.com	An excellent website explaining internet safety for children, parents and teachers
www.saferinternet.org.uk	The UK Safer Internet Centre
www.thinkuknow.co.uk	CEOP's Thinkuknow website
www.internetmatters.org/wp-content/uploads/2016/07/E-safety_Pre_School.pdf	E-safety tips for parents of pre-school children
www.internetmatters.org/wp-content/uploads/2016/07/E-safety_11_13_YearOlds.pdf	E-safety tips for parents of 11-13 Year Olds
www.internetmatters.org/wp-content/uploads/2016/07/E-safety_Primary_School.pdf	E-safety tips for parents of primary school children6-10 Year Olds
www.internetmatters.org/wp-content/uploads/2016/07/E-safety_Teenagers.pdf	E-safety tips for parents of teenagers 14+ Year Olds

10. Use of School Wi-Fi on Personal Devices

The School provides a wireless network which staff and visitors may use to connect their mobile devices to the internet. Access to the wireless network is at the discretion of the School which may withdraw access from anyone who it considers is using the network inappropriately. Use of the network is at their own risk. The School will have no liability whatsoever for any loss of data or damage to the user's personal device resulting from use of the School's wireless network. The network requires users to configure certificates on their personal device for security and monitoring purposes. The School uses technology which detects and monitors the use of mobile and other devices that are connected to or logged on to the wireless network.

By using a mobile device on the School's IT network, staff and students agree to such detection and monitoring. The School's use of such technology is for the purpose of ensuring security of its IT systems and safeguarding purposes.

For and on behalf of the Governors
D.A.P. King

Appendix A

Chigwell School Biometric Information

Biometric information is information (data) about a person's physical or behavioral characteristics that can be used to identify them. Examples include, but are not limited to, finger pattern, face recognition, iris recognition.

Government Legislation
Government legislation, The Protection of Freedoms Act 2012, which was effective from September 2013, requires that written parental permission is obtained to use pupils' biometric data.

This legislation requires schools to:

- Inform parents about the use of the biometric systems in the school and explain which applications use biometrics
- Receive written permission from one parent for the school to process biometric information for their child
- Ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system if a parent or pupil has objected
- Allow children to choose an alternative way of being identified if they wish

Further details can be found at https://www.gov.uk

Biometric Information at Chigwell School
Chigwell will record a biometric measurement taken from a finger (not a fingerprint image). The information is converted into a unique digital signature that is stored on a database. Chigwell will use the finger pattern biometric authentication of pupils for the purposes of a secure locker system.

Frequently asked Questions

How does it work?
When your child places his/her finger on the scanner, the software matches their finger pattern image with the unique digital signature held in the database, and access to the appropriate system is granted.

What about security?

- The biometric signature that is stored cannot be used to recreate an image of the child's fingerprint
- The data is held securely in compliance with the Data Protection Act 1998 and cannot be used by any other agency for any other purpose
- The school will not use the biometric information for any purpose other than as stated above

What happens when my child leaves the School?
The biometric data is permanently deleted when your child leaves the school.

Why are you asking for my permission?
Due to the recent changes in legislation, schools which already have automated biometric recognition systems in place now or are introducing new systems have a duty to obtain consent in order to process their child(ren)'s biometric data for any purpose.

Do I have to give permission for each system?
Yes, we must obtain written consent for each system. If you object to only one of the systems then please make that clear when completing the consent form or objecting.

What if I object?
By law, we must notify each parent of a pupil under the age of 18 if we wish to take and use biometric data as part of an automated biometric recognition system. As long as the child or a parent does not object, the written consent of only one parent will be required. If either parent objects, the other parent's consent will be overridden. You may also withdraw your consent at any time in writing.

What if my child objects?
Unlike their parents, a child does not have to object in writing. A pupil's objection or refusal overrides any parental consent to the processing. We recommend that you discuss your child's rights with them.

What will the school do if I or my child has objected?
The school will ensure that the data is not taken/used as part of the system they object to. If the data has already been collected then the data will be deleted.

What happens if the School introduces another biometric system?
The school is obliged to inform parents of each and every system that uses biometric data. Therefore, the school will write to you with full details and a new consent form.

What happens next?

In order for pupils to take advantage of using the biometrics system as detailed above, we enclose a consent form for you to sign and return. We would ask that you sign and return this consent to the School.

Please note without this consent form we will be unable to take a template of your child's finger pattern.

Appendix B

Pupils' Use of ICT Agreement

- I know that the School can remotely monitor what I do on school and personal devices connected to the School Wi-Fi, e.g. my email, internet use, documents and printing.
- I will keep my password to myself – I will not let anyone else use it, and I will not use theirs.
- I will be aware of my personal safety when I am communicating online, and I will not share personal information about myself or others.
- I will tell a teacher immediately about any unpleasant or inappropriate material or messages on the computer, or anything that makes me feel uncomfortable when I see it.
- I understand that the School's security and internet filter is there to protect me, and protect the computer network, and I will not try to bypass it.
- I understand that I must not use VPNs, proxy servers, or any other tools to bypass the School's internet filter and monitoring systems, as these protections are in place to keep me and others safe online.
- I know that I must respect others when using the computers/tablets.
- I will not use the computers/tablets to harass or bully anyone.
- I will be polite online, and I will not use strong, aggressive, or inappropriate language. I appreciate that others may have different opinions.
- I will not take or distribute pictures or videos of anyone without their permission.
- I will not physically damage School computers or change settings on the computer that will leave it broken for the next person.