



E-SAFETY POLICY

REFERENCE:	V01 – 09/2025
OWNERSHIP:	AP Lead
AUTHORISED BY:	Emma Draper (Director)
REVIEW:	Annually – September 2026

PURPOSE

The purpose of this policy is to the responsibility to educate our students on e-safety issues; teaching them appropriate behaviour and skills to enable them to remain both safe and legal whilst using technology for learning or socially.

This policy aims to highlight some of the issues associated with ICT and provides guidance on how ICT should/could be used.

SCOPE

This policy applies to The Churchwood Forest School AP School (TBS), this includes all employees who work within Churchwood Forest School AP as well as contractors, volunteers and visitors.

SAFEGUARDING COMMITMENT

As an organisation that prioritises the safeguarding of children and all vulnerable people, The Churchwood Forest School AP School is committed to providing a safe environment across all we do by actively adopting strategies that embed a culture of zero tolerance for abuse of any kind.

RESPONSIBILITIES

As e-safety is an important aspect of strategic leadership within the centre, the Provision Lead and Education Leadership Team/Directors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All members of the Churchwood Forest School AP School community need to be aware of the key people responsible for e-safety. At least one member of the Provision leadership needs to have undertaken training by a recognised organisation to deal with issues relating to e-safety and to allow training to be given to staff.

There is an expectation that Provision Leads and provision staff regularly access this policy on an annual basis. It is their duty to ensure they have an understanding of the issues and strategies at their Centre in relation to local and national guidelines and advice.

This policy, supported by the centre’s acceptable use agreements for staff, visitors and students, is to protect the interests and safety of the whole Churchwood Forest School AP School community.



It is linked to the following mandatory centre policies: Safeguarding, Health and Safety, Student Conduct Agreement, Behaviour and Anti-Bullying, as well as being linked to the PSHE curriculum.

DEFINITIONS

For our provision's e-safety policy, e-safety encompasses the comprehensive practice of using information and communication technologies (ICT) – including the internet, mobile devices, and various digital platforms – in a manner that is responsible, safe, and ethical. It's about more than just preventing harm; it's also about empowering everyone in our community to make the most of the opportunities the digital world offers, securely and confidently.

This policy aims to educate and equip students, staff, and parents with the knowledge and skills necessary to navigate online environments effectively. It addresses crucial aspects such as identifying and mitigating risks like cyberbullying, where digital technologies are used to harass or intimidate; online grooming, which involves adults building relationships with children for exploitative purposes; and exposure to inappropriate content, including violent, sexual, or otherwise disturbing material.

E-safety covers vital areas like understanding data privacy, ensuring personal information is protected, and recognizing misinformation and fake news, which can spread rapidly online. By implementing robust e-safety measures and fostering an informed approach, our goal is to create a positive, protective, and empowering online experience for every individual within our school community. This proactive stance helps us ensure that everyone can engage with technology safely and productively.

POLICY GENERAL PRINCIPLES

Introduction

Technology plays an important role at Churchwood Forest School AP School . It is often used within lessons as a central resource to help with the educational development of our students. Furthermore, it helps with the administrative side of our work with young people and is key to all online learning taking place across our Churchwood Forest School AP School Centres.

However, whilst the educational possibilities of using ICT are rapidly developing, all users of technology need to be alert and responsive to the potential dangers and risks associated with its use. These include:

- content: being exposed to illegal, inappropriate or harmful content; for example: pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation



and extremism.

- contact: being subjected to harmful online interaction with other users; for example: peer on 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; 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.

At Churchwood Forest School AP School , we understand the responsibility to educate our students on e-safety issues; teaching them appropriate behaviour and skills to enable them to remain both safe and legal whilst using technology for learning or socially.

Social Networks

Facebook, Twitter, Snapchat, Instagram, TikTok, YouTube, WhatsApp, online gaming and other forms of social media are increasingly becoming an important part of our daily lives. However, students often misuse social networks, including by sexually harassing their peers via their mobile and smart technology, sharing indecent images: consensually and non- consensually (often via large chat groups), and viewing and sharing pornography and other harmful content. In addition, there is an increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the internet.

We teach safe, responsible use (privacy, reporting, blocking, misinformation/disinformation) within the curriculum. Concerns about harmful online content or contact are reported to the DSL the same day; criminal or immediate-risk matters follow NPCC ‘When to call the police’ thresholds.

Therefore, the use of social networks at Churchwood Forest School AP School Centres is not allowed and students take part in lessons highlighting the risks when using the internet and social networks in their own time.

Staff are not permitted to access their personal social media accounts using Churchwood Forest School AP School equipment during working hours. If staff are using Churchwood Forest School AP School equipment to access social media outside of work hours, they must be mindful of the fact that data will be stored locally within the device history, that they need to log out at the end of



the session and that login details should not be auto-filled or remembered by the device.

Students are not permitted to access their social media accounts whilst at the centre on ANY device be it Churchwood Forest School AP School equipment or that of their own.

Staff, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

Staff, students, parents and carers are aware that the information, comments, images and videos they post online can be viewed by others, copied and stay online forever.

Staff, students, parents and carers are aware that their online behaviour should at all times be compatible with law.

Staff should not befriend current students on social networking sites and best practice is to wait until that student is 19 before doing so.

Staff are not permitted to post any information or images regarding students or their centre on social media using their private accounts. Any posts for Churchwood Forest School AP School should be made on the relevant Churchwood Forest School AP Group pages by Churchwood Forest School AP Communication Team, this can then be shared by others when available.

It is recommended that all staff who have private social media accounts change their usernames to ones where their identity can't be easily identified and privacy settings should be set to the maximum protection.

Mobile and Smart Technology

Students may bring mobile telephones or smart devices to the [provider name but they must be switched off and handed in to staff at the beginning of the school day. As an AP, Churchwood Forest School AP does not have school statutory search powers. Where a prohibited/unsafe item or content is suspected, staff seek voluntary handover or consent to check outer clothing/bags. If consent is refused and there is immediate risk or a suspected offence, staff secure the area and contact police per NPCC 'When to call the police'. Staff do not examine digital content; they preserve evidence and inform the DSL and the commissioning school/LA the same day.

Students may be permitted to have their phones or devices back for a specified period within the lunch break to check for messages, provided they are then handed back to staff until the end of the day. Students are not permitted to access social networks on their devices during this time and



staff should provide an adequate level of supervision to ensure this does not happen. The privilege of having access to their phone or device during lunchtime will be withdrawn for any student that does not comply with this expectation. There should be no need for students to make or receive calls from their mobiles in the Centre – all phone calls should be made or received on the [provider name] Phone.

Deleted[m]:] School UK Centre

Use of the Internet - including Filtering

Staff and students are able to access a wealth of information via the Internet to help with education/study. It is important though that the Internet is not used excessively and is well planned into the curriculum. The Churchwood Forest School AP provides students with supervised access to Internet resources through the use of appropriate filtering software. Websites and their content are filtered by software and provisions can add to the list of blocked sites flexibly and quickly. Churchwood Forest School AP's IT support provider centrally controls this.

Staff should preview any recommended sites before use to check that they work on the centre system and are appropriate, including checking that they do not contain any terrorist or extremist material.

Raw image searches are discouraged when working with students and key search terms are provided to students.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/carers recheck these sites and supervise this work. Parents/carers will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute Churchwood Forest School AP-owned software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

The Internet should be used primarily for educational purposes. Where students are given permission to use the Internet recreationally, close supervision must be given to the sites they are visiting and content they are viewing.

Should you come across a website that is inappropriate it is important to alert IT support to these to allow the website to be blocked across the organisation and in the short-term, to block it locally. If you wish to access a website that is blocked centrally, you may request for this to be unblocked, again by contacting IT support. This website will be checked and a request sent through to the



provision lead to confirm acceptance of this.

There should be no attempt to access sites deemed inappropriate as this may trigger an alert on the monitoring system. If any student uses the Internet inappropriately, this should be logged with the Provision Lead and the E-safety Lead should be made aware of all significant or ongoing concerns.

Monitoring

Authorised ICT support staff may access ICT equipment that is owned/leased by the centre at any time with prior notice.

In certain circumstances, the Provision Lead or a member of the Education Leadership Team/Directors may instruct the service provider to monitor, intercept, access, inspect, record and disclose emails, instant messaging, internet/intranet use and any other form of electronic communication involving any student or employee, without consent, to the extent permitted by law.

Occasions where this may be necessary include:

- Confirming or obtaining centre business-related information
- Confirm or investigate compliance with centre standards, policy and procedures
- Quality control or training purposes
- Prevent or detect crime
- Child protection

All monitoring, investigative and surveillance work should be conducted by authorised ICT staff and comply with the Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 and the Lawful Business Practises Regulations 2000.

All Internet activity is filtered by Churchwood Forest School AP's internet provider. Browsing history will be monitored by the Centre. Churchwood Forest School AP uses appropriate software to filter internet use and to view and control student computer use.

Acceptable Use Agreements

Each year, ALL staff employed at Churchwood Forest School AP shall undertake some training with regard to e- safety. As part of this training, all employees should sign an Acceptable Use Agreement and this must be held by the Provision Lead.

All students should take part in one dedicated lesson at the start of the year (or when they start at



the centre) where e-safety is addressed and students re-sign an Acceptable Use Agreement.

A copy of the staff, student and parent/carer agreements can be found in the appendices of this policy.

Parents/carers should be alerted to the e-safety policy during the referral interview, through the referral form and it should be made available as a hard copy or electronically if requested. The E-Safety policy and additional information related to e-safety is accessible from the Churchwood Forest School AP website. Parents/carers should sign the AUP and read the E-Safety policy during the referral interview before their child starts at Churchwood Forest School AP. They should also be aware of and give consent to any guidance for online distance learning e.g. all meetings will be recorded.

E-Safety in the curriculum

E-safety is securely embedded into the curriculum. It is essential for students to receive the same message across all staff and to learn the skills necessary for staying safe using ICT. Below are some areas covered in the curriculum.

Staying Safe online in each of the 4 areas of risk (content, contact, conduct and commerce) and also recognising and guarding against radicalisation:

- Social Networks
- Cyberbullying
- Sexual harassment
- Sexting or Youth Produced Sexual Imagery
- Copyright and keeping information safe and secure
- Legislation relating to computers and technology
- Respecting information
- Using correct appropriate search techniques
- Cross Curricular E-Safety

ICT now plays a key part in the education of students. ICT is used widely for research and to enhance the quality of work produced by students. It is important that teaching and learning incorporates the use of ICT and that when planning and delivering lessons using ICT, matters relating to e-safety are considered by all staff.

Staff Training



Training will be provided annually to all staff as part of the introduction to the new academic year. This will be focussed on keeping students safe and managing risk. Regular information on e-safety will be provided to staff to keep staff abreast of developments. Over the academic year, there may be opportunities for staff to attend additional training events. Information about these will be published when available. All staff will review the Acceptable Use Agreement on an annual basis and sign the document to acknowledge their professional responsibilities in relation to ICT in general. New staff starting midyear will need to sign this as part of their induction.

Churchwood Forest School AP Email System - Staff

The use of email within Churchwood Forest School AP is an essential means of communication for staff. In the context of Churchwood Forest School AP, e-mails CANNOT be considered as private and should therefore only be used for official [provider name business.

Churchwood Forest School AP gives each member of staff an email account in order to protect staff and minimise the risk of receiving malicious/unsolicited emails.

All email may be filtered and logged and email histories may be re-traced. Therefore, it should only be used for official Churchwood Forest School AP business.

Users should keep passwords and account details secure.

Students/parents/carers should, under no circumstances, be contacted by staff using their personal email address.

Emails should be carefully checked before sending as any content signifies official Churchwood Forest School AP correspondence, similar to that of letters being sent using letter headed paper.

Emails created on an Churchwood Forest School AP account may be disclosed where required by law (e.g., data-protection requests or legal proceedings) and may be shared with the commissioning school/LA for safeguarding or compliance. Churchwood Forest School AP is not a public authority under FOIA; data is handled under GDPR/Data Protection Act 2018.

Staff MUST inform their line manager and Designated Safeguarding Lead (DSL) of any offensive emails they receive.

Send emails to intended recipients only. Do not send blanket emails unnecessarily.

Only send attachments to intended recipients.

Check emails regularly and delete unwanted items.



Never open attachments from unwanted/unknown sources.

Email for Churchwood Forest School AP Students

Churchwood Forest School AP provides a dedicated in-house email system for students using Outlook via Office 365. When students start in the centre, they will be assigned a Churchwood Forest School AP email address through Outlook/Office 365 account for use in online learning, ICT lessons and the wider curriculum. Students may not use these until they have covered safe use of the Office 365 system in a dedicated ICT lesson. Students may also use email accounts provided by their referring schools should they need to.

Student users are expected to adhere to general good practice guidelines of netiquette (delivered in e-safety lessons). Language should be appropriate and they should not reveal any personal information about themselves to other people.

Students should be aware that all email may be filtered and logged and email histories may be re-traced, therefore it should only be used for Churchwood Forest School AP learning and school work.

Churchwood Forest School AP gives each student an email account in order to protect students and minimise the risk of receiving malicious/unsolicited emails.

Students should keep passwords and account details secure.

Emails should be carefully checked before sending as any content signifies official Churchwood Forest School AP correspondence, similar to that of letters being sent using letter headed paper.

Emails created on a Churchwood Forest School AP account will be subject to disclosure should a request be made under the Freedom of Information Act 2000.

Students MUST inform their Provision Lead and/or Designated Safeguarding Lead of any offensive emails they receive. Where an email may contain illegal content or child sexual abuse material, staff/DSL will follow national guidance (e.g., CEOP/police) and preserve evidence; students must not forward or download such content.

Check emails regularly and delete unwanted items.

Never open attachments from unwanted/unknown sources.

Use of Digital Images and Video



Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images of any member of the Churchwood Forest School AP community or the public, without first seeking consent and considering the appropriateness.

Not all parents/carers give permission for photographs of students to be taken. This information can be found on referral forms and must be adhered to as there are often safeguarding reasons why photographs should not be taken and used.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. Only centre-owned devices configured by the Churchwood Forest School AP may be used to take photos within the [provider name, with recorded consent (or another lawful basis) and a clear purpose. Images are transferred to secure storage the same day and deleted from the capture device. Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the .

Where digital images/photographs are used and shared publicly, no identifying detail should be used, unless strictly necessary and risk-assessed (avoid names, uniforms, badges, geotags); only share where a lawful basis exists and consent/preferences are honoured.

For the protection of all involved, online lessons may be recorded where a DPIA identifies this as necessary and proportionate; access is restricted; retention follows the Churchwood Forest School AP Data Protection Policy; parents/carers and the commissioning school are informed of the approach.

Misuse of ICT

Complaints of Internet Misuse must be reported and dealt with by the Provision Lead, the E-Safety Lead, or the Designated Safeguarding Lead (DSL). Incidents involving the creation/possession/sharing of 'nudes and semi-nudes' or suspected illegal content are escalated to the DSL immediately; do not view or copy content. The DSL will follow local procedures and, where appropriate, CEOP/police routes.

Any complaints about staff misuse should be directed to the Provision Lead or the Education Leadership Team/Directors.

Complaints of a child protection nature should be referred in the usual manner to the centre-based Designated Safeguarding Lead.



Reviewing Online Safety

Churchwood Forest School AP’s E-Safety Lead will carry out an annual review of our approach to online safety, which will be supported by an annual risk assessment that considers and reflects the risks our students face. Issues arising from this will be incorporated into written policies and procedures and addressed during annual staff training. The review will evidence compliance against DfE Filtering & Monitoring Standards, roles/responsibilities for filtering/monitoring, and staff training updates required by KCSIE 2025.



POLICY CONTEXT

AP Standards Addendum (AP): Churchwood Forest School AP operates as an Alternative Provision (AP). Commissioning schools/LAs retain statutory responsibilities for attendance registers and sanctions; Churchwood Forest School AP provides same-day safeguarding/attendance information to enable those duties. Online safety: DSL holds lead responsibility; our filtering/monitoring aligns with DfE Filtering & Monitoring Standards and KCSIE 2025. Searches: Churchwood Forest School AP does not have schools’ statutory search powers; we use consent-based checks and involve police using NPCC ‘When to call the police’ thresholds where risk/offences are suspected.

This policy relates to the following legislative requirements, standards and internal documents:

Legislation & Standards	• DfE statutory guidance – Keeping children safe in education, September 2025 • General Data Protection Regulations 2018 • The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 • Regulation of Investigatory Powers Act 2000 • Human Rights Act 1998 • Racial and Religious Hatred Act 2006 • Sexual Offences Act 2003 • Communications Act 2003 (section 127) • The Computer Misuse Act 1990 (sections 1 – 3) • Malicious Communications Act 1988 (section 1) • Copyright, Design and Patents Act 1988 • Public Order Act 1986 (sections 17 – 29) • Protection of Children Act 1978 (Section 1) • Obscene Publications Act 1959 and 1964 • Protection from Harassment Act 1997 • General Data Protection Regulations 2018 • The Freedom of Information Act 2000
Related Forms & Documents	• Acceptable use agreements for staff, visitors and students • Safeguarding Policy • Health and Safety Policy • Student Conduct Agreement • Behaviour and Anti-Bullying Policies

VERSION CONTROL

We will review our documentation regularly and we reserve the right to amend our policies and procedures at any time.

Version	Date	Change Summary	Author/Reviewer	Approved by:
1	23/09/2025	Initial Version	Mark Wrangles	



2				
3				