WESTFIELD PRIMARY SCHOOL

ICT and Internet Acceptable Use Policy

This Policy was written by K Beattie/ A Newport

November 2025

Review: September 2026

Designated Safeguarding Lead ("DSL")	Julia Findlay
Computing (ICT and Online Safety) Lead:	Kate Beattie

Westfield Primary School
ICT and Internet Acceptable Use Policy

Introduction
At Westfield Primary School, we are committed to fostering a safe and enriching learning environment through the effective and responsible use of ICT, the internet and computing technologies. This policy outlines the acceptable use of ICT and internet resources to support teaching, learning, and maintaining professional conduct while safeguarding the school, its staff, and its pupils.

Purpose
This policy aims to ensure the safe and secure use of school ICT resources by all users, including students, staff, volunteers, governors and visitors. In particular to:

- Ensure staff and pupils benefit from ICT tools and internet access while adhering to safe and acceptable use guidelines.
- Protect the school from inappropriate use of ICT resources that could bring it into disrepute or harm its reputation.
- Provide guidance on the professional use of school equipment, email, internet, and mobile technologies, including personal devices used for school business.
- Outline responsibilities for safeguarding data, protecting privacy, and promoting a positive and safe online environment.

It outlines the rules and guidelines that users must follow when using school ICT resources.

1. General ICT and Computing Use

1.1 Professional Use:

- ICT facilities, including remote access, must only be used for professional purposes or reasonable personal use as agreed by the Headteacher or Local Advisory Committee.
- The use of school systems or devices for illegal, offensive, or inappropriate purposes, including but not limited to engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any way is prohibited.
- Any and all school business must only be carried out using the email addresses that are part of the secure school system. All communication with parents and other stakeholders must be compatible with a professional role. Any queries regarding this must be raised with SLT.
- Any incidents of concern regarding children's safety must be reported following the school's child protection and safeguarding policy and procedures.
- Staff should also be aware of their obligations under the Staff Behaviour (Code of Conduct) policy.

1.2 Password Security and Privacy:

- All activity carried out under a staff member's username is their responsibility. Staff must ensure that they log out or lock devices when not in use.
- staff must:

(i) choose strong passwords. The School's IT team advises that a strong password:
  - contains at least 8 characters.
  - contains numbers and special characters (!£$*#).
  - avoids using common passwords such as school name, staff members name, etc.

(ii) keep passwords secret;
(iii) never reuse a password;
(iv) change their passwords regularly;
(v) never disclose passwords or allow unauthorized users to access school systems.

In case of password compromise, staff must change their password immediately and inform Eduthing and the Headteacher or School Business Manager.

1.3 Email Communication and the Internet:

- Every member of staff has an email account. This should be used for any work-related emails. Each class is also assigned a school email address, all of which have the same password.
- Staff must only use school-provided email accounts for all work-related correspondence.
- Communications must be professional and free of content that could be misinterpreted.
- Communications must not contain personal opinions about other individuals, e.g. other staff members, children or parents.
- The school system (including emails) must only be accessed using school devices. School data and information must not be accessed using personal devices. This is with exception of the Headteacher and Designated/Deputy Designated Safeguarding Leads who may use personal devices to support the school when needed. School Chromebooks and laptops are available upon request.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be sent using Egress wherever possible or encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the School Business Manager immediately and follow our data breach procedure.

- Staff must ensure that they set an appropriate out of office message to both internal and external contacts during school holidays. This must give clear dates of closures and state the email box will not be monitored, in line with GDPR procedures.
- Staff must use school email and internet services for educational and school-related purposes only. The use of personal email addresses by staff for any official school business is not permitted.
- Staff must not use school email or internet services to harass, intimidate, or defame others.
- Staff must not use school email or internet services to send spam, viruses, or other harmful content.

1.4 Online Conduct:

- Online activity, including social media use by staff both in school and outside of school, must not bring their professional role or the school into disrepute. Staff should avoid discussing or engaging with school matters on personal social media accounts.
- Security settings on staff personal social media accounts should be set to the highest level. For support with how this can be achieved see the Computing Lead.
- For further clarification, staff should refer to the school's Social Media policy.

1.5 Data Protection:

- Personal data, such as pupil information, must be kept secure and only accessed remotely with authorization. Unauthorized sharing or mishandling of such data is prohibited.
- All removable media must be encrypted and used only in extenuating circumstances as approved by the Computing Lead or Senior Leadership Team.
- All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

1.6 Remote Working:

- Staff must comply with the school's remote working policies and procedures.
- Staff must ensure that their home or remote working environment is safe and secure.
- Staff must use school-provided equipment and resources when working remotely.
- School data must not be stored on a home computer, or un-encrypted storage device.
- When working off-site, school devices must be stored in a secure location, such as a locked office or room. Devices must not be left unattended in public spaces or areas with high foot traffic, and staff must ensure that device screens are locked when not in use.

2. Use of School Devices

2.1 General Guidelines:

- All school devices (e.g., laptops, Chromebooks, cameras) are the property of the school and must only be used for school-related work.
- Laptops and Chromebooks taken home should only be used by staff members and not partners or other family members.
- Staff should take all reasonable precautions to prevent loss or theft of school-owned devices, including keeping them secured and in a safe location when not in use. Portable devices are insured by the school at home and in transit to school but are not covered if left unattended in vehicles or unsecured locations. If they are stolen from the classroom, they will not be covered by insurance unless there is evidence of a break in.
- Wherever possible, staff must use the remote server to complete work at home. USB sticks must be encrypted and provided by school, but should only be used in extenuating circumstances after discussion with the Computing Lead, Kate Beattie or a member of the Senior Leadership Team.
- No external device should be connected to the school's ICT network without approval from the Computing Lead or a member of the Senior Leadership Team.
- If school resources such as email/ authentication devices are configured on a personal device, they must have 2fa set up for secure access. Staff are required to report any loss or theft of the personal device to eduthing and the Headteacher or SBM immediately, so remedial action can be taken.
- Staff must not tamper with or modify any school equipment or resources without permission from Eduthing.
- Any lost or stolen school-owned devices must be reported to Eduthing and the Headteacher or School Business Manager immediately to prevent unauthorised access to sensitive data or breach of security.

2.2 Installation of Hardware, Software and Updates:

- Only hardware, software applications and updates approved by an authorised member of the school's IT support team at Eduthing may be installed on school devices. Staff must not introduce unauthorized software to school systems.
- Staff will respect copyright and intellectual property rights.

2.3 Virus Protection & Firewall Security:

- All school devices are protected by regularly updated antivirus software. Staff must exercise vigilance when downloading files or opening email attachments. Where a file or email is derived from a source outside of school it should be subjected to a virus scan before opening a document.
- Staff must keep their school-provided devices updated with the latest anti-virus and firewall software.

- Staff must not disable or modify any anti-virus or firewall software without permission from the school's IT support team at Eduthing.

2.4 Monitoring:

- Internet use and device activity are monitored using Sensocloud by the Lead DSL. Any inappropriate or suspicious activity will be flagged and reviewed by the Lead DSL or Headteacher.
- The school reserves the right to monitor and log all staff user activity on the school's ICT resources. Staff must be aware that for safeguarding purposes, they have no expectation of privacy when using the school's ICT resources.
- The school reserves the right to delete suspect e-mail; e-mails containing inappropriate material or references, or containing attachments, which are inappropriate or containing viruses.
- Staff should not use websites or mechanisms to bypass the school's filtering or monitoring mechanisms.

3. Taking and Storing Photographs of Pupils

- Only school devices should be used to take photographs of pupils and only after ensuring these adhere to the photo permissions granted for each child.
- No photographs or digital recording should be taken of pupils using personal devices in any circumstances.
- Images of pupils should not be distributed outside the school network without explicit authorization from the headteacher.
- Photos for the website or press must only include the child's first name.

4. Social Media and Online Safety

- The school's social media accounts (e.g., X/Twitter) are moderated by the Computing Lead. Responses to messages must be approved by SLT before posting.
- Staff must actively promote online safety to pupils, fostering responsible use of digital tools and social media.
- The School has a Social Media policy which should be read in conjunction with this policy.

5. Reporting and escalation procedures for security incidents and breaches:

- All staff must report any security incidents or breaches immediately to Eduthing and the Headteacher or School Business Manager.
- The school's cybersecurity incident response policy must be read and complied with by all staff in the event of a security incident or breach.
- Staff must cooperate fully with Eduthing in investigating and resolving security incidents and breaches, including providing any necessary information or access to affected devices or accounts

6. Sanctions for Misuse

- Disregarding this policy may result in disciplinary action as per the school's procedures. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.
- Staff must be aware that the use of ICT leaves a digital footprint that can potentially identify them, regardless of whether the incident occurred on a home computer, school computer, or mobile phone. Misuse of ICT can be a criminal offence under various laws,
- Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the school considers may amount to a criminal offence, or is unlawful, shall without notice to the user concerned, be reported to the police or other relevant authority.
- Accidental access to inappropriate material should be reported to the Lead DSL immediately.
- Staff alleged to have accessed or stored inappropriate material will be subject to investigation under the school's safeguarding policies. The Headteacher & Lead DSL must consider the allegation and determine the appropriate way forward. (see Allegations of Abuse Against Staff Policy).
- The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Acknowledgement
By signing this policy, I confirm that I understand and agree to comply with the provisions outlined above and will support the safe and effective use of ICT and the internet across the school.

I agree to report any perceived or known misuse of the network to the Headteacher or School Business Manager. Moreover, I agree to report any websites that are available on the school internet that contain inappropriate material to the Headteacher or School Business Manager. I agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Headteacher or School Business Manager.

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to dismissal. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the school will monitor activity in order to uphold this policy and to maintain the integrity of the school's network.

Full Name: _____

Job Title: _____

Signature: _____

Date: _____