



Gardners Lane &
Oakwood Federation

Acceptable use of IT,
Technology and Data
Protection Policy

Approved July 2026
Review July 2027

This policy applies to all staff, volunteers, governors, contractors and regular visitors working for the Gardners Lane and Oakwood Federation, including any school-provided devices, personal devices used for Federation work, cloud services, email, learning platforms and social media accounts when used for school business. It complements the Federation Safeguarding Policy and Data Protection (GDPR) procedures.

Roles and Responsibilities:

- ☐ Headteacher: overall responsibility for policy implementation and resourcing.
- ☐ Data Protection Officer (DPO): oversees GDPR compliance, leads any data breach response and advises staff – usually a Governor
- ☐ Designated Safeguarding Lead (DSL): assesses safeguarding risks from digital incidents and coordinates child protection responses.
- ☐ IT Lead: implements technical controls (antivirus, filtering, device configuration), investigates suspected security incidents and maintains device inventory.
- ☐ Governors: ensure appropriate oversight of data protection and online-safety arrangements via termly reports.
- ☐ All staff: follow the policy, complete mandatory training and report incidents promptly.

The Federation fosters a protective environment where the safety and security of our children, families, pupils, users and staff is our highest priority.

Due to the ever-changing landscape of technology and the modern threats that have arisen over the last few decades, it is necessary to continually adapt Federation policies and procedures to maintain these high standards.

The Acceptable Use of IT, Technology and Data Protection policy represents a commitment across the whole Federation to work together to keep our children, families, pupils, users and staff safe, as well as to uphold the wider goal of protecting sensitive personal data.

This is to ensure that our children, families, pupils, users, parents, staff and governors / directors can feel confident that their information is handled responsibly with the same care that we would wish to see applied to our own sensitive personal information.

Accessibility:

Key elements (parental consent forms, privacy notices, attendance/online-safety communications) will be made available in accessible formats and translated into key community languages on request. Staff should support parents/carers with understanding digital consent.

By signing below this policy, you agree to the following

1. I will take reasonable precautions to protect my password:
 - a. I will never share my password with anyone. Where I believe that another individual has discovered my password, I will immediately inform IT.
 - b. I will not make a written note of my password unless it is stored securely.
 - c. I will not choose a password that can be easily guessed.
 - d. I will not choose a password which I have used outside of the Federation.
2. I will take reasonable precautions to protect the passwords of pupils or other users:
 - a. I will not allow pupils or other users to share or know each other's passwords.
 - b. I will not keep a record of pupils or other users' passwords. If I need to look one up, I will access the password via the systems established by the School.
3. I will take the appropriate action when I or another individual has come into contact with harmful material:
 - a. If the nature of the material is inappropriate for the Federation context or might have a detrimental effect on the individual viewing it, I will immediately inform a member of the senior management team.
 - b. If the nature of the material poses a risk to the security of the computer network, or if I am unsure of its nature, I will immediately inform a member of IT and seek advice.
 - c. If the material is of an illegal nature, I alert a member of the Senior Management Team who will contact the police.
4. I will maintain a professional manner when using any Federation provided communication systems. (email, mobile phone, computer, laptop etc)
5. I will take reasonable precautions to protect images captured at, or for, the Federation:
 - a. I will never use a personal device to take pictures of the Federation or its children, families, pupils, users and staff.

- b. I will never publish an image taken at the Federation, or of its children, families, pupils, users and staff, unless I have obtained permission from a member of the Senior Management Team.
- c. Where a child or pupil has taken sensitive images of themselves or others, I will not delete the images but instead confiscate the device and deliver it immediately to the Designated Safeguarding Lead.

Images and consent:

- Photographs and videos of pupils may only be taken/stored/used where there is a lawful basis. For identifying images published externally (website, social media), explicit written parental/carers consent is required and recorded in the school's consent register.
- Storage and retention: images must be stored on Federation systems only and retained in accordance with the Data Retention Schedule; personal devices must not hold school images.
- Deletion/confiscation: where a child creates or shares sensitive images, staff must confiscate the device, secure it and hand to the DSL; staff must not view or delete images except under DSL guidance.

- 6. During Remote Learning, we have seen children working remotely and sending pictures to staff showing what they have been up to whilst out of the classroom.

- a. I will use my professional judgement before using any pictures shared with school by a parent/carers depicting activities pupils have engaged in whilst out of school. For example, it is not appropriate to upload a picture of a child who is wearing swim wear or who is wearing revealing clothing.
- b. I will ensure the use of any pictures shared with school by parents/carers have the relevant parental permission before being shared on our school website or Class Dojo.

- 7. I will take reasonable precautions to avoid potentially compromising online activity.

- a. I will not access social networks whilst working unless pre-approved to use them as part of my role or for educational purposes.
- b. I will only communicate with children, families, pupils, users and staff using Federation approved systems.

- c. I will not engage in any online activity which may compromise my professional responsibilities.
- d. **Misinformation and Disinformation:**
 - **Misinformation:** False or misleading information shared without harmful intent.
 - **Disinformation:** Deliberately false information shared to deceive or manipulate.
 - Applies to all digital communications, including emails, social media, messaging apps, and online platforms accessed via school or personal devices.
 - Staff must fact-check before sharing and use vetted sources. Where staff suspect harmful disinformation affecting pupils or the school's reputation, report to SMT/Communications Lead. SMT will coordinate corrections, parental communications and, if needed, regulatory/legal advice.

Staff Responsibilities

- Staff must **not knowingly share or promote misinformation/disinformation** through any school-related communication channels.
- Staff are expected to **model critical thinking and responsible digital behaviour** for pupils.
- Any content shared with pupils must be **fact-checked and sourced from reputable platforms**.

Teaching and Learning

- Schools should integrate **digital literacy education** to help pupils identify misinformation online.
- Staff should encourage pupils to **question sources**, verify facts, and understand bias in digital content.
- Use of **AI tools, social media, and search engines** should be guided by principles of accuracy and ethical use.

Monitoring and Reporting

- Any suspected spread of misinformation or disinformation should be **reported to the designated safeguarding lead (DSL)** or online safety coordinator.
- The school may monitor digital communications to ensure compliance with this policy.

Monitoring and filtering:

The Federation uses internet filtering and monitoring tools to protect pupils and staff. Monitoring includes email, device activity on school-managed devices and access logs.

Monitoring is carried out for safeguarding, security and policy compliance. Staff should have no expectation of privacy when using Federation systems.

Where monitoring involves personal data, the DPO has documented the lawful basis and data protection impact assessment (DPIA) on file.

Incident reporting and response:

Online-safety concerns (e.g., sharing of inappropriate material, grooming): report immediately to the DSL via CPOMS and follow DSL instructions.

Data breach: report to the DPO and SLT immediately, complete the Data Breach Form within 24 hours. The DPO will lead assessment and, where required, notify the ICO within 72 hours.

IT security incidents: report to IT Lead immediately. Do not switch off devices unless advised.

Recording and escalation: all incidents will be logged centrally; DSL/DPO will determine next actions, including parental contact, police referral and ICO notification.

Consequences

- Breaches involving misinformation/disinformation may result in **disciplinary action**, especially if they compromise safeguarding, reputation, or pupil wellbeing.

8. I will take reasonable precautions to separate my professional and private life:

- a. I will not use my personal device for Federation work unless I have prior approval from my Line Manager and my personal device has been approved by IT.
- b. **Smartwatches are permitted** for staff in most schools but **must be used responsibly**.

Their use is typically **restricted during contact time** with pupils to avoid distractions and maintain professionalism.

Camera, messaging, and internet functions should be **disabled or not used** when staff are working directly with children.

Key Guidelines

During Teaching or Contact Time:

Smartwatches should be used **only as timekeeping devices**.

Functions like notifications, calls, or messaging should be **turned off or silenced**.

Staff should **not interact with smartwatches** unless in an emergency.

Privacy and Safeguarding:

Staff must **not use smartwatches to take photos or videos** of pupils.

Personal data or school-related information **must not be accessed or stored** on smartwatches.

Any wearable device with recording capabilities must be **used with caution** and in line with data protection policies.

Break Times and Non-Contact Periods:

Use of smartwatches is generally allowed during **breaks or in staff-only areas**.

Staff should ensure that **pupils are not present** when using smartwatches for personal reasons.

Professional Boundaries:

Staff should **not share smartwatch contact details** with pupils or parents.

Communication with parents or pupils should be conducted via **official channels** only.

Policy Enforcement:

Breaches of smartwatch use policy may lead to **disciplinary action**.

Staff are expected to **model appropriate technology use** for pupils.

I will not use my personal email for Federation communication.

I will not use my Federation email for personal communication.

9. I will not attempt to bypass or remove antivirus or content filtering systems from any Federation device.
10. Where it comes to my attention that children, families, pupils, users or staff have discovered a flaw in the Federations digital security systems, I will inform IT and SLT immediately.
11. I will not use removable storage media, such as encrypted memory sticks, unless pre-approved by my line manager and only for exceptional circumstances.
12. If I take a Federation device offsite, I will not allow anyone else to use it.

13. I will adopt a conscientious approach to data protection, and follow all Federation guidance in relation to GDPR compliance, and keep the rights of the data subject in mind at all times:

- a. I will only share sensitive data within the confines of the Federation with colleagues where there is a legitimate need.
- b. I will only share sensitive data outside the confines of the Federation when:
 - i. I have a justifiable and legitimate need to do so.
 - ii. I have removed any unnecessary information.
 - iii. I am confident that the agency / third party I am sharing the data with will take the necessary steps to protect it and complies with GDPR guidance at all times.
- c. If I believe there has been a data breach I will follow the Federations “data breach” guidance and inform the relevant person as soon as possible and complete the data breach form within 24 hours.

D. All staff must complete mandatory online-safety and data protection training on induction and annually thereafter. Records will be kept by HR. All staff must sign this Acceptable Use Agreement on induction and re-sign after substantive policy updates.

14. I understand that if I do not follow the guidance contained in this policy, I may be subject to disciplinary action.

Name	
Signature	
Date	