Springwell School

ICT Policy

Last review: September 2026

Next review: September 2027

Name: **Dan Kronbergs**

Position: **IT Network & Digital Transformation Manager**

Hinkler Road, Thornhill, Southampton, SO19 6DH
023 80 445 981

Contents

Introduction and Aims 3

ICT Provision 3

Equipment 3

Software 3

Internet 4

Microsoft Apps 4

Web access platforms 4

Phones 4

CCTV 4

Asset recording 4

Online Safety 5

Internet Use for children and young people with SEN – Introduction 5

Teaching and Learning 5

Introducing Online Safety to the pupils 5

Infrastructure security 5

E-Mail 6

Pupils' images 6

Managing Emerging Technologies 6

Assessing risks 6

Reports on network filtering & monitoring 6

Handling Online Safety complaints 6

Preventing Radicalisation 6

Social Media 7

Introduction 7

Expectations for the use of social media 7

GDPR & Data Protection 8

Use of Artificial Intelligence (AI) Tools 9

Introduction 9

Expectations for the use of AI Tools 9

Acceptable Use – Pupil 10

ICT Acceptable Use Agreement– Staff 11

Introduction and Aims

Springwell School has excellent ICT provision for both staff and pupils. The use and education of ICT is promoted to children of all ages and abilities.

This policy sets out the type of technology used within the school, the boundaries of acceptable use for staff and student and how ICT is delivered. **The policy concludes with an acceptable use policy sign off page which must be completed by all staff or acknowledged via School's relevant platform, eg. National College.**

ICT Provision

Equipment

The school regularly invests in ICT equipment and as a result has an outstanding ICT infrastructure across the school including:

- Physical servers & network switches
- Virtual server environment
- Site wide wireless network
- ID card door access management
- VoIP Telephony
- Printing services
- Teacher & Pupil Mobile Devices
- Trolleys of mobile devices, such as pupil laptops and iPads
- Appropriate software applications for pupils & staff
- ICT Suites for pupils
- Staff workrooms
- Interactive whiteboards
- Staff laptops for teachers
- Remote Access for staff

All ICT equipment is managed by the Springwell IT Helpdesk. The school have a rolling replacement plan based on age of equipment, usability, and warranty, this ensures ICT is always current and operational.

Software

All equipment is loaded with a Springwell School build for consistency, this enables seamless working of digital media across the school system. This is managed by Springwell IT Helpdesk.

Internet

The school has a DfE “Filtering & Monitoring standards” compliant internet feed outsourced by

Broadband4 & SchoolCare. Any device connected to school network can have its network traffic monitored. Any guest devices can utilise the school guest network, but some websites maybe blocked and not working as expected due to enhanced filtering. The network gateway is protected by firewalls, secure tunnels, and filters. The school can manually block sites if necessary. This service is annually reviewed for suitability. To support the DfE standard mentioned, the school has implemented additional filtering with instant notifications and reports to relevant staff members- Senso Cloud. This is managed by Springwell IT Helpdesk.

Microsoft Apps

Teaching and support staff have school Microsoft accounts, this provides cloud-based Email, calendars, an online storage drive and many more of the Office 365 apps. Email usage can be monitored and should only be used for work purposes. This is managed by Springwell IT Helpdesk.

Web access platforms

Teaching and support staff have access to various teaching, learning, incident, administration platforms, such as School MIS Arbor, NeoPeople, PlusPay, Tapestry, CPOMS and many others. These are managed by various departments and school staff members, whilst the Springwell IT Helpdesk can direct to the right point of contact.

Phones

Springwell School use a VOIP phone system for the main school site and in satellite classrooms. Calls are effectively managed through a call routing system. All calls made to or received by, external numbers are recorded and can be monitored for safeguarding purposes. This is managed by Springwell IT Helpdesk.

CCTV

Parts of the school site is covered by CCTV both externally and internally where there is a need to deter criminal damage and protect children. The data is retained for a reasonable amount of time and is reviewed only with good reason. Springwell School use this data for internal review of incidents and to provide training with permission of its staff. This is managed by Springwell Site team while backed up by Springwell IT Helpdesk.

Asset recording

Springwell IT Helpdesk manages and maintains the ICT asset register which is reviewed regularly. All mobile devices such as laptops, iPads and smartphones have got their locations and dedicated “owners” recorded. Any loan devices are managed via the “School Booking” system in shared areas, while staff can borrow a laptop from the IT Team for short duration. This would be recorded via the Helpdesk. All school devices can be monitored and locked, while iPads and smartphones can be remotely tracked and wiped if they go missing. Staff must report broken or missing equipment as soon as possible. This is managed by Springwell IT Helpdesk.

Online Safety

- The school's Online Safety Co-ordinators are:
    - Data Protection Officer
    - IT Manager

Internet Use for children and young people with SEND – Introduction

Pupils with SEND are potentially more vulnerable and more at risk than others when using ICT:

- Those Pupils with ASD may make literal interpretations of content which will affect how they respond.
- They may not understand some of the terminology used.
- Those with complex needs do not always understand the concept of friendship and therefore trust everyone implicitly. They may not know how to make judgements about what information is safe to share. This leads to confusion about why you should not trust others on the internet.
- Some pupils may be vulnerable to bullying through the internet or not recognise that they are being bullied.
- They may not appreciate how their own behaviour may be seen by someone else as bullying.

In order to protect the Pupils at Springwell School, we have put the following measures in place:

Teaching and Learning

The school has a duty to provide Pupils with suitable internet access as part of their learning experience. It is also part of the statutory curriculum and a necessary tool for staff and pupils. Springwell School ensures that:

- Pupils must be always supervised by a staff member, while using ICT equipment
- The school internet service is designed expressly for pupil use and includes filtering appropriate to the needs of our pupils.
- Pupils will be taught, as part of the computing curriculum, what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet.

Introducing Online Safety to the pupils

- Online Safety is explained in a format appropriate for our pupils during:
    - PSHE Lessons as part of the curriculum
    - Annual "Safer Internet Week".
    - Computing curriculum content where appropriate

Infrastructure security

- School ICT systems, capacity, and security are reviewed annually and as soon as any known security threat has been identified.
- Anti-Virus protection is updated automatically.
- Additional anti-malware protection is updated automatically.
- Security strategies outlined by the National Cyber Security Centre are being reviewed and followed as necessary.
- Removable media is disabled across the network.
- Anonymous external Sharing via SharePoint & OneDrive is disabled.

E-Mail

- Pupils are not given their own email accounts on the school system.

Pupils' images

- Photographs that include pupils will only be used for school use according to the Springwell Media Management Privacy Notice.
- Written or online signed permission from parents or carers for the use of photographs on the external use is requested as part of the annual data collection process.

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.

Assessing risks

- The school will take all reasonable precautions to ensure that users only access appropriate 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. If staff notice inappropriate ads or content, they will immediately alert IT team to investigate and disable or block in future.
- The school will audit ICT provision to establish if the Online safety policy is adequate, and that the implementation is effective.

Reports on network filtering & monitoring

- Allowed websites and URLs on school filtering are being reviewed annually.
- Wherever applicable, the DSL may request a filtering report from the Springwell IT Helpdesk
- There is an additional layer of filtering which provides instant notifications to relevant staff numbers regarding any suspicious activity.

Handling Online Safety complaints

- Any complaints of internet misuse will be dealt with by the IT Manager.
- Any complaints of a child protection nature will be dealt with in accordance with school child protection and safeguarding procedures.

Preventing Radicalisation

This policy only contains the technical steps put in place for Prevent. Further information can be found in the schools safeguarding policy.

- The school's internet feed has been specifically filtered to block the following categories to assist with preventing radicalisation: Terrorism, extremism and violence.

Social Media

Introduction

The school seeks to achieve an appropriate balance in the use of social networks by staff as private individuals, but also as employees and educators, with professional reputations and careers to maintain, and contractual and legislative requirements to adhere to. Whilst the School does not wish

to discourage staff from using such sites on the Internet in their personal time, it does expect certain standards of conduct to be observed to protect the school and its reputation, and also to protect staff from the dangers of inappropriate use. Accessing social networking sites in working time and/or from School ICT equipment is strictly forbidden, whether the equipment is used at home or at school.

This policy section relates to the use of social networking applications by School staff in their own personal time, using their own ICT equipment.

Expectations for the use of social media

Working in an educational setting with young people, staff have a professional image to uphold, and how individuals conduct themselves online, helps to determine this image.

- The School prohibits staff from accepting invitations to "friend" pupils, or pupil's family members/friends.
- Staff must not initiate friendships with pupils, or pupils' family members/friends, under any circumstances.
- Staff who maintain social networking friendships with work colleagues, are required to adhere to the requirements below relating to the content of their interactions.
- Staff must not refer on social networking sites to the School, its employees, pupils, and their families. If staff adhere to this recommendation, then the personal content of an individual's social networking memberships is unlikely to be of concern to the School. If employment at the School is referred to, then the information posted would need to comply with the conditions set out below.
- Any references made to the School, its employees, pupils and their families, should comply with the School's policies on conduct/misconduct, equal opportunities, and bullying and harassment.
- Staff must not post information on a social networking site which is confidential to the School, its employees, its pupils or their families.
- Staff must not post entries onto social networking sites which are derogatory, defamatory, discriminatory or offensive in any way, or which have the potential to bring the School into disrepute.
- Staff should not use the School logo on their own personal social networking accounts, and should not post any photographic images that include pupils or members of staff.
- Staff must not publish copyrighted or confidential information including materials created for the school.
- Staff must not express personal views which could be misinterpreted as those of the School or City Council
- When posting any information onto a social networking site, staff must not post any entry that puts their effectiveness to perform their normal duties at risk.
- If individuals feel aggrieved about some aspect of their work or employment, there are appropriate informal and formal avenues, internally within the School, which allow staff to raise and progress such matters. Social networks are not the appropriate forum to raise such matters. Employees should discuss any concerns with their head teacher/line manager in the first instance. Guidance is also available from HR/Payroll and trade unions.

Security and privacy

Staff are advised to check their security profiles and privacy settings on the social networks that they use. If individuals are not clear about how to restrict access to their content, they should regard all content as publicly available and act accordingly. If you require any assistance, please contact Springwell IT Helpdesk.

In using social networking sites, staff are recommended to only post content that they would wish to be in the public domain.

Policy breaches:

Staff found to be in breach of this policy may be subject to disciplinary action, in accordance with the School's Disciplinary Policy & Procedure and the Code of Conduct and Disciplinary Rules, with potential sanctions up to and including dismissal. Information shared through social networking sites, even on private spaces, is subject to copyright, data protection, freedom of information, equality, safeguarding and other legislation. Where staff work in roles that are governed by professional bodies/professional codes of conduct; the professional rules relating to social networking applied to them may be more stringent that those within this Policy.

GDPR & Data Protection

Springwell is committed to keeping staff, pupil, and parent's data safe. The school has a staff and pupil privacy notice, which details what and how data is stored and processed. It can be found on our school website and please see our **GDPR & Data Breach policy** for more information.

Staff are expected to follow the below to ensure data is kept safe:

- Data must not be removed from the school server or School SharePoint.
- The use of USB sticks is prohibited unless permissions has been granted by the IT Manager.
- Passwords must be kept confidential and password manager used where possible.
- Multi-factor authentication enabled for main school work account and 3rd party platforms, where possible.
- Thought should be given about what type of information is used, when creating a display.
- Computers should be locked whilst unattended.

Data breaches must be reported in line with the data breach policy.

Use of Artificial Intelligence (AI) Tools

This section outlines the acceptable use of Artificial Intelligence (AI) tools, specifically Microsoft Copilot Chat, within our school. It aims to ensure that AI is used responsibly, ethically, and in a manner that enhances learning and administrative processes. It applies to all staff who use Microsoft

Copilot Chat for school-related activities. Staff accounts are secured by enterprise data protection during usage of Microsoft Copilot Chat.

The school reserves the right to monitor the use of AI tools to ensure compliance with this policy.

Introduction

1. **Educational Enhancement**: AI tools could be used to support and enhance educational experiences but should not replace traditional teaching methods.
    - *Example*: Staff can use Microsoft Copilot Chat to support lesson planning but should still engage with pupils through discussions and hands-on activities.

2. **Ethical Use**: All users must adhere to ethical guidelines, ensuring AI is used in a manner that respects privacy, promotes fairness, and avoids harm.
    - *Example*: Staff should not use AI to generate inappropriate, harmful, offensive content or false information about someone to bully in any form of communication

3. **Compliance**: Users must comply with all relevant laws, regulations, and school policies when using AI tools.
    - *Example*: Staff should ensure that any AI-generated content complies with copyright laws and does not plagiarize existing materials.

Expectations for the use of AI Tools

- **Confidentiality**: Staff must not input any confidential or sensitive data into AI tools.
    - *Example*: Do not enter any personal information, such as personal pupil information or medical records into Microsoft Copilot Chat.

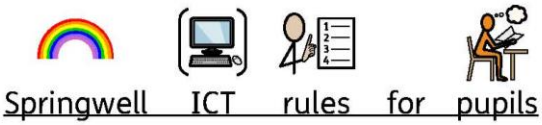
- **Data Protection**: Follow the school's data protection policies and guidelines to ensure the security of personal data.
    - *Example*: Use secure channels for any necessary data transfers and ensure that AI tools are used in compliance with GDPR.

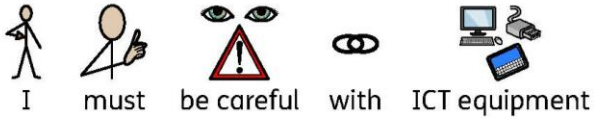
- **Awareness**: Be aware of the data that AI tools collect and how it is used.
    - *Example*: Understand that AI tools may collect usage data to improve their services, and ensure this data is handled according to privacy

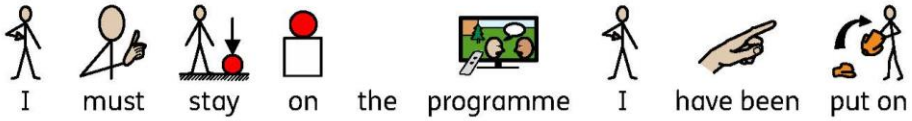
laws.# Acceptable Use – Pupil

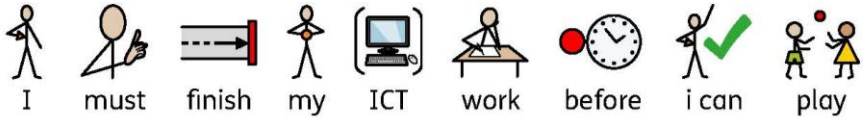
Given the range of needs and nature of the children at Springwell School an acceptable use policy for Pupils is presented in symbolised format. Staff guide and educate pupils on what is and isnot

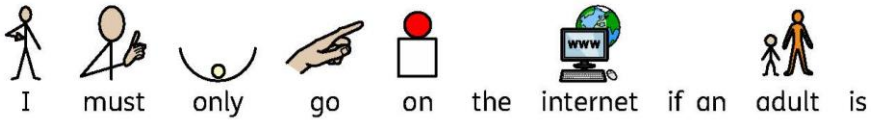
acceptable constantly with the use of icons and pictures. Pupils ICT rules below:

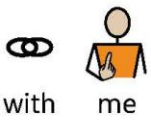


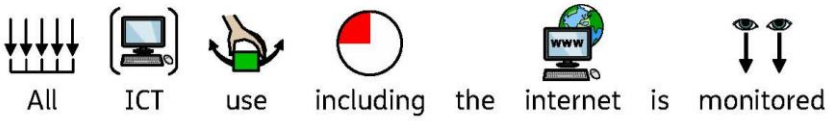












ICT Acceptable Use Agreement– Staff

The use of ICT is encouraged at Springwell School. The school has a responsibility to protect the schools and users from abuse of the systems. **Staff must read, agree, and adhere to the rules set out below and in the whole ICT policy.**

1) Access

1.01 Staff have access to computers, laptops, smartphones and tablets within school.
1.02 Staff will be issued with a username and password for the school domain.
1.03 Staff must not share their password with anyone.
1.04 Staff must set a suitable password, at least 8 characters long, lower-case, upper-case, numbers, and special characters. Passwords will be reset only during certain scenarios, such as: data breach, unauthorized access, forgotten password, after using a public network, using someone's personal device.
1.05 Staff will be prompted to set up Multi factor authentication using a personal mobile device or number.
1.06 Staff will use different passwords for different platforms and use Edge password manager where possible.
1.07 All files stored on the school systems must be work related.
1.08 All work-related data must be stored on the school-owned devices and school network (any day-to-day data, which does not contain sensitive or confidential information can be stored via Office365 services, for example: Teams, SharePoint, and OneDrive).
1.09 Sensitive & confidential data must be stored on the school devices & network only. Remote access is provided to work off site.
1.10 Personal USB keys, SD cards and optical media (CD/DVD) must not be used for school data.
1.11 Teachers have remote access via VPN to work off site on school network.
1.12 School owned devices will have access to the wireless network.
1.13 Staff may have access to the Guest wireless network for personal purposes.
1.14 Use AI to assist with lesson planning, assessment, and administrative tasks.
1.14.1 *Example*: A teacher can use Copilot to draft a lesson plan outline, which they can then customize to fit their teaching style and class needs.
1.15 Ensure that AI-generated content is reviewed and validated before use.
1.15.1 *Example*: Before sharing AI-generated materials with other people, staff should review the content for accuracy and relevance.

2) Computer Security

2.01 I will use the ICT equipment with care.
2.02 I will not tamper with any ICT equipment including cables.
2.03 I will report broken or faulty equipment to Springwell IT Helpdesk.
2.04 I will not install software onto the school system without permission from the Springwell IT Helpdesk.
2.05 I will never give anyone my login details.
2.06 If I think someone knows my login details, I will update my password immediately and inform Springwell IT Helpdesk.
2.07 I will not leave a computer logged in unattended.
2.09 I will not access data I am not authorised to.

3) Email

3.01 I understand my user@springwellschool.net email is for work use only.
3.02 I will only use the approved school email account for school communication.
3.03 I will only open email attachments from known trusted senders.
3.04 I will choose a suitable password and keep this private.
3.05 I will not forward chain letters containing sensitive data.

4) Monitoring

4.01 I understand all access to the school network is logged and monitored.
4.02 I understand all files and emails on the school system are property of Springwell School and therefore system administrators have the right to access them if required.
4.03 I understand emails use and contents can be monitored.
4.04 I understand the school records all its phone calls and they are reviewed only with good reason.
4.05 I understand the school has a CCTV system and footage is retained for safety of pupils and staff, recordings can only be accessed with good reason.
4.06 I understand the school may wish to review and show CCTV recordings for training.
4.07 I understand school issued phone or tablets can be tracked and remotely managed for security purposes.

5) Data Protection

5.01 I will not share School data including images externally without approval.
5.02 I will be aware what is classed as 'personal data' and will not share this.
5.03 I will not project or display 'personal data'
5.04 I will not store school data on my personal computer or mobile device.
5.05 I will use the VPN Connection only to access and work on school data.
5.06 I will avoid inputting confidential and sensitive personal data into AI tools.

6) Inappropriate Use

6.01 I will not share private information about another person.
6.02 I will not post malicious or defamatory information about the school.
6.03 I will not post media of students or staff on social media.
6.04 I will not access material that's profane or obscene.
6.05 If I access inappropriate material by mistake, I must report this to the Springwell IT Helpdesk immediately.
6.06 I will not take photos or videos of pupil using my own ICT equipment.
6.07 I will not use AI to generate inappropriate, harmful, offensive content or false information about someone to bully in any form of communication.

I have read and understand all the rules and guidelines in the ICT policy and Acceptable use section for Staff. I understand failure to comply could lead to disciplinary action.

Name: _____

Job Role: _____

Signature: _____

Date: _____