



Statement of Policy for Acceptable Use of ICT including e-Safety

Introduction

For clarity, the policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc. Wider school community – students, all staff, governing body and parents.

Safeguarding is a serious matter; at All Saints Anglican/Methodist Primary School, we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is two-fold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the All Saints Anglican/Methodist Primary School website. At the beginning of each academic year, a general review as part of training days will ensure all staff understand the policy and adhere to Staff Acceptable Use (Appendix 1). A summary of this policy and Students' Acceptable Use Policy will be signed at the beginning of each year.

Roles & Responsibilities

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least bi-annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of safeguarding at the school who will:
 - Keep up to date with emerging risks and threats through technology use.

- Receive updates from the head teacher in regards to training, identified risks and any incidents.
- Feedback to full Governing Body where appropriate.

Head Teacher

Reporting to the governing body, the head teacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to the e-Safety Officers, as indicated below. The head teacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officers have had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officers

The day-to-day duty of e-Safety Officers is devolved to Lisa Richmond, Sally Nicholson and Education Lincs. The e- Safety Officers will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head Teacher.
- Advise the governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make themselves aware of any reporting function with technical e-safety measures, i.e. Internet filtering reporting function; liaise with the responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Mac OS X (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officers and Head Teacher.
- Passwords are applied correctly to all users regardless of age. It is recommended that passwords for staff be a minimum of 8 characters.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head Teacher.
- Any e-safety incident is reported to the e-Safety Officers (and an e-Safety Incident report is made), or in their absence to the Head teacher. If you are unsure the matter is to be raised with the e-Safety Officers or the Head teacher to make a decision.
- The reporting procedures in this policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and information/links on the school website the school will keep parents up to date with new and emerging e- safety risks.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy when joining the school before any access can be granted to school ICT equipment or services.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to

staff following induction and understanding staff Acceptable Use; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Students are permitted to use the school email system, and as such will be given their own gmail address.

Visual Images – Use of digital media visual images are covered in the schools' Photographic Permissions. All parents will sign a visual images release slip included in the New Starter Pack; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; All Saints Anglican/Methodist Primary School is supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within All Saints Anglican/Methodist Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officers who will advise the Head Teacher for a decision to be made. Any new service will be risk assessed before use is permitted.

Twitter – used by the school as a broadcast service.

Remote learning due to COVID -19 – Where required and in line with government advice for remote learning, the school will provide a digital curriculum which may include but not limited to links to secure learning platforms, websites, applications and digital worksheets.

In the case of live or pre-recorded lessons, staff will strictly follow guidance in order to keep themselves and other parties safe from breeches of confidentiality and/or safeguarding issues. Communication between school and parents/children will only be made through the correct and monitored channels

In addition, the following is to be strictly adhered to:

Permission slips (via the Photographic Permissions) must be consulted before any image or video of any child is uploaded to our website. No identifiable photos of children will be used on Social Media. There is to be no identification of students using first name and surname; first name only is to be used. Where services are “comment enabled”, comments are to be set to “moderated”, where possible.

All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take-down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use

that resource, it will be removed within one working day of the school becoming aware.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officers, or in their absence the Head Teacher. The e-Safety Officers will assist you in taking the appropriate action to deal with the incident and to fill out an incident log on the school's current system.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, All Saints Anglican/Methodist Primary School will have an annual review which is suitable to the audience.

e-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officers are responsible for recommending a programme of training and awareness for the school year to the head teacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head Teacher for further CPD.

Reviewed September 2024

Next Review September 2025

Appendix 1 Acceptable Use – Staff

Note: All Internet and email activity is subject to monitoring
You must read this statement in conjunction with the above Policy.

USE OF E-MAIL AND INTERNET (including Social Media)

It is the responsibility of a school to ensure that all users use e-mail and Internet service in an acceptable manner and in accordance with the schools acceptable use policy and any e-mail and Internet agreements established by the school. Schools should use Nottinghamshire County Council's email and Internet code of practice for schools to establish their own policies on the acceptable use of email and internet.

The Internet provides users with access to worldwide information services, bringing new opportunities for communication. With the increasing popularity of social media tools such as Facebook and Twitter thought should be given when using these tools for publishing information about a school.

Social media tools are excellent tools for teaching and learning and can provide exciting, new opportunities for schools to engage, communicate and collaborate with users and the wider community.

Whilst social media tools can provide tremendous benefits to schools they also have serious security risks in their use. Risks such as people posting unsafe or inappropriate information about themselves and their personal lives online as well as providing opportunities for offenders to groom and exploit children. In order to mitigate these security risks and still enjoy the benefits of social media schools should establish and enforce good social media usage policies which should include the following points:

- Supervision in the classroom with social media technology must be appropriate to the children's needs and abilities;
- It is good practice for staff to evaluate websites before classroom use. Staff should be aware that websites, search results etc. may be safe and appropriate one day but unsafe a day later. All members of the school community should be aware that filtering software is not always effective and cannot always be relied on alone to safeguard children;
- Children with Special Educational Needs should be appropriately supported according to their specific needs and their personal understanding of the e-Safety risks;
- All pupils and staff should be aware of the school procedure regarding what to do if inappropriate content or messages are found, sent or received online;
- All pupils and staff should understand how to critically evaluate online content;
- Internet filtering must be in place according to the school's requirements. This should be designed with both a technical and curriculum focus and should be agreed by the schools Leadership Team and Governors;
- ICT tools provided by the school should always be used (e.g. work provided digital cameras, memory cards, laptops etc.) rather than personally owned equipment.

Social networking – is allowed in school in accordance with this policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. It is acceptable for staff to 'like' and/or share school social media content but they are advised to refrain from comment. It is advised that staff members' personal accounts protect their privacy. Staff should not become 'friends' with pupils on personal social networks under any circumstances. Staff would not normally 'friend' parents except where there is an existing link outside the professional setting.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

PASSWORDS

The school is responsible for establishing and enforcing a password policy for its use of ICT. The Head Teacher is responsible for establishing and enforcing a password policy on their systems based on the level of security required. Passwords must be assigned to individual users of ICT systems to maintain security and the data that they contain.

Appropriate:

- Users only using their own account to carry out day to day work;
- Users not disclosing their password to allow others to access their account. Users should be aware passwords are for the benefit of the school and are the proprietary and confidential information of the school;
- Users selecting a password that is easy to remember but not for others to guess;
- Users not selecting obvious passwords, such as the name of a close relative, friend or pet;
- Compliance with the password policy for each computer system.

Inappropriate:

- Requesting passwords personally assigned to other users;
- Using a session via another users password;
- Sharing passwords with other users. All users must take reasonable precautions to protect their passwords;
- If a user thinks that their username or password has been used without their permission, they must change the password and inform the head teacher as soon as practically possible. The head teacher will ensure that new users are issued with appropriate usernames and passwords. When a user leaves their job, whether leaving the school or not, the head teacher will ensure that all usernames and passwords for that user are suspended as appropriate.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pen-drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Elston All Saints Anglican Methodist Primary School recognise that staff choose to access school information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.

School will support and enable staff to ensure that their devices are compliant.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Encryption protection will be available for staff and suitable advice provided.

Appendix 2 – Own Device Usage Acceptance must be signed by all staff.

USE OF PCs, LAPTOPS & SERVERS

Appropriate:

- Storing school data;
- Loading text, images, video or audio streams in connection with day to day work activities;
- Storing limited amounts of personal data (where agreed by the head teacher).

Inappropriate:

- Loading unauthorised or untested software;
- Allowing unauthorised users to access laptops used away from school;
- Failure to keep laptops used away from school secure;
- Storing confidential or personal data or information on removable media without adequate protection or encryption;
- Deliberate, reckless or negligent introduction of viruses;
- Storing personal material protected by copyright which has not been purchased;
- Loading files containing pornographic offensive or obscene material.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Viruses and other malware - any virus outbreaks are to be reported to the Education Lincs Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

THE LEGAL FRAMEWORK

ICT use in a school setting should be legally regulated, this includes the content of e-mail, or sites downloaded from the Internet; privacy issues, monitoring of communications and surveillance at work and employment relations. Further legal advice should be sought, if appropriate, from Council's Children and Young people's Services HR or Legal Services.

If the school monitors e-mails or scans for profanity/inappropriate content then users should be warned of this through policies.

Appendix 2 – Own Device Usage Acceptance

Staff - Acceptable Use of Personal Devices

Elston All Saints Anglican Methodist Primary School recognise that many staff choose to access school information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.

School will support and enable staff to ensure that their devices are compliant.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Encryption protection will be available for staff and suitable advice provided.

Own device usage agreement

I understand and accept that should I choose to access school data on any personal device that I use or own must have, and use, suitable encryption to secure the data.

Any unlawful access of data on such a device will be my responsibility. I will report any theft or loss to the School Business Manager or Head Teacher as soon as is practicable.

When exchanging, gifting, upgrading or selling the device I shall ensure that access to any school data is removed and data that relates to school is securely deleted.

Name:

Signed:

Dated: