

E-safety policy

Introduction

At St Aidan's we have a diverse, balanced and creative approach to employing electronic technology across most subject areas, but we are acutely aware of the potential problems children can find themselves in. We ensure all our staff and children understand these risks and know how to avoid them. All pupils are taught about e-safety and staff are committed to keeping this important subject a topical issue.

This policy should be read together with other related school policies: *Safeguarding and child protection, Behaviour, Anti-bullying and Data protection.*

Contents

1	Aims and objectives	2
2	Definitions	2
3	Roles and responsibilities	2
4	Electronic communication with the school	4
5	Servers, passwords and data security	4
6	Mobile phones and other portable devices	5
7	Social media and online discussion	6
8	Photographs and videos	6
9	Cyber-bullying	7
10	Working online	8
11	Acceptable use of the internet in school	8
12	Use of work devices outside school	8
13	Education, advice and training	9
14	Pupils' online safety education	9
15	Staff training	10
16	Dealing with infringements	10
17	Review	11
18	Glossary	11
	Appendix 1: ICT acceptable use agreement – EYFS & KS1	12
	Appendix 2: ICT acceptable use agreement – KS2	13
	Appendix 3: ICT acceptable use agreement – adults	14

1 Aims and objectives

The aim of this policy is to protect everyone involved in the school from being a participant in or the victim of, illegal, offensive or harmful activities associated with modern electronic media.

- 1.1 This policy lays out the acceptable use of computers, cameras, mobile phones and other portable devices in a way that can be understood and adhered to by everyone involved in the school. (See also our *Data protection policy*.)
- 1.2 It also aims to establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- 1.3 Failure to comply with this policy may lead to disciplinary procedures.

2 Definitions

- 2.1 Portable devices include smartphones, tablets, laptops and mp3 players.
- 2.2 Social networking sites are those such as Facebook, YouTube, X (formerly Twitter), Snapchat, Roblox etc.
- 2.3 As identified in *Keeping Children Safe in Education* (2023), our approach is based on addressing the following categories of risk.
 - a. **Content**: being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism and terrorist material.
 - b. **Contact**: being subjected to harmful online interaction with other users, such as peer-to-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.
 - c. **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm, such as 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.
 - d. **Commerce**: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

3 Roles and responsibilities

- 3.1 **The Governing Body (GB)** has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. Regular meetings are held with appropriate staff to discuss online safety and online safety logs, provided by the Designated Safeguarding Lead (DSL) are monitored. All governors will:
 - ensure that they have read and understand this policy;
 - agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3);
 - ensure that teaching about online safety is appropriately adapted for vulnerable children, victims of abuse and some pupils with SEND.
- 3.2 **The Headteacher** is responsible for:
 - ensuring that staff understand this policy, and that it is being implemented consistently throughout the school;

- e-safety is included in the Child Protection training;
- staff are fully trained in E-safety and the GDPR.

3.3 **The Designated Safeguarding Lead (DSL)** takes lead responsibility for online safety in school, which includes:

- supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- working with the Headteacher, ICT technician and other staff, as necessary, to address any online safety issues or incidents;
- managing all online safety issues and incidents in line with the school's *Safeguarding and Child Protection policy*;
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's *Behaviour policy*;
- updating and delivering staff training on online safety, liaising with other agencies and/or external services if necessary;
- providing regular reports on online safety in school to the GB.

3.4 **The lead teacher for Computing** is responsible for monitoring the effectiveness of this policy and ensuring that e-safety is taught regularly to all children.

3.5 **The ICT technician** is responsible for, amongst other things:

- putting in place an appropriate level of security protection, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school;
- ensuring that the school's ICT systems are secure and protected against viruses and malware and that such safety mechanisms are updated regularly;
- monitoring the school's ICT systems and conducting full security checks on a weekly basis;
- blocking access to potentially dangerous sites and, where possible, preventing potentially dangerous files from being downloaded.

3.6 **All staff and volunteers**, including agency staff, are responsible for, amongst other things:

- maintaining an understanding of this policy and implementing it consistently;
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3) and ensuring that pupils follow the school's terms on acceptable use (Appendices 1 or 2);
- working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's *Behaviour policy*;
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, maintaining an attitude of 'it could happen here'.

3.7 **Parents** are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy;
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 or 2).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#);
- Hot topics– Childnet International;
- Parent resource sheet– Childnet International;
- Relationships– Disrespect Nobody

3.8 **Visitors and members of the community** who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 3).

4 Electronic communication with the school

Children do not have school email addresses.

4.1 Teachers have school email addresses which are only used for internal communication.

- If parents wish to email queries they should do so to the office manager (admin@staidansprimaryschool.org.uk) who will confidentially pass them on to the appropriate member of staff.

4.2 Each year group has a dedicated school email address for general communication about children's work.

4.3 Parents and carers are signed up to our text messaging service which is frequently used to distribute information.

4.4 In order to reduce paper usage and to communicate more effectively with parents, we use e communication wherever possible: general information, including the Headteacher's fortnightly newsletter, *Headlines*, is sent to parents electronically. Paper will continue to be used only where return slips are required or recipients have no access to the internet.

4.5 We publish a lot of information on our website (www.staidansprimaryschool.org.uk) and we aim to keep this updated regularly. Information such as policy documents and *Headlines*, can be found here.

5 Servers, passwords and data security

The licensed software we use for administration and the filtering systems we use to block viruses and inappropriate material are security checked and approved by LGfL (London Grid for Learning).

5.1 Some websites and servers require passwords when logging on. Children are taught the importance of always keeping these strictly to themselves.

5.2 There are three servers at the school, each with increasing levels of restriction:

- a. a pupil server for which all children and staff have passwords;
- b. a staff server for which staff only have passwords;

- c. an administration server, restricted to the administrators and Senior Leadership Team.
- 5.3 All classroom staff have passwords to the external LGfL server giving access to a wide range of services.
- 5.4 All staff regularly change the passwords they use to access the school network to ensure security.
- 5.5 Children automatically have LGfL email addresses, which, together with their log-ins, give them the potential to access individual blogs and LGFL content from home and school to work on specific fixed-term projects.
- 5.6 Supply teachers and other visiting teachers are given a dedicated password that allows them to use our software without compromising security of our servers.
- 5.7 Data is held securely and is handled sensitively and appropriately. Our servers are automatically backed up every week onto an external hard drive which is stored in a fire-proof safe.
- All school business is conducted through secure LGfL email accounts.
 - When working on documents containing sensitive information (eg. reports or LSPs) on classroom computers, teachers must ensure their displays are set to computer only.
 - Teachers must not download pupils' personal data onto their own computers.
- 5.8 Any data breaches must be reported to the Headteacher in the first instance and then to the DPO as required.

6 Mobile phones and other portable devices

Children are not allowed their personal mobile phones or other portable devices at school. If any such device is brought into school it must be left in the office in the morning and may only be collected in the afternoon at the end of the school day. Staff may bring in mobile phones or other portable devices for their own use but may only use them during breaks or non-contact time. At all other times these must remain switched off and be kept in a locker or bag. Other adults visiting during school hours are asked to comply with this rule.

- 6.1 If a member of staff has a family emergency they may either seek permission from the Headteacher to keep their mobile phone to hand or they may use the school's or their own phone to make calls from the staff room or the school office.
- 6.2 The school has a number of mobile phones for use during school trips. If staff use their own mobile phones, they must block their number before contacting parents. Parents attending these trips must not use their personal mobile phones when with the children.
- 6.3 Staff must not use their mobile phones either to contact current pupils or store their telephone numbers and personal details on them except in exceptional circumstances. In such cases the express permission of the Headteacher is required.
- 6.4 Tablet computers are widely used in school. The children are supervised when using portable devices that can access the internet. The LGfL filtering system ensures safe, appropriate content.

- 6.5 It is absolutely forbidden to bring any portable device into school containing inappropriate or illegal material.

7 Social media and online discussion

Children do not have unsupervised access to these sites at school.

- 7.1 All staff at St Aidan's are strictly prohibited from:
- publishing, viewing or commenting via any form of social media during work hours or from the school's facilities;
 - disclosing any information regarding children or staff (written or pictorial), and other confidential information regarding the school, even in private messages to other members of staff;
 - using the school's name for social media identities, log-in IDs and user names without prior approval from the Headteacher;
 - using the school's logo on any internet posting unless they are doing so on behalf of the school with clear permission from the Headteacher or Chair of Governors.
- 7.2 When engaging in online discussions, staff are expected to
- make it clear that the opinions and views expressed are solely those of the author and do not necessarily represent the views of the school management or other staff;
 - always exercise good judgement and common sense regardless of whether online comments relate to their job;
 - respect copyright, privacy, fair use and other applicable laws.
- 7.3 Staff must not post comments that can be interpreted as:
- illegal activity;
 - offensive, personal attack or defamation;
 - bullying and harassment;
 - spam.

8 Photographs and videos

At the beginning of each year, along with the home school agreement, we seek permission for the use of photographs and videos of children on our website, in newsletters and other publications. Parents who change their minds about permitting publishing privileges should inform the school in writing. All staff are aware of the list of children for whom we do not have such permission.

- 8.1 Photographs and videos of children are not published on sites other than the school's own website without express permission from the Headteacher.
- 8.2 It is essential that all photographs are deemed suitable – great care must be taken not to make children feel uncomfortable or embarrassed; pictures of children in toilets or undressing are forbidden.
- 8.3 If we caption children in photographs we only ever identify them by their first names.
- 8.4 The school's cameras should be used to record school events, trips, classroom activities and work. Photography must be carried out either by, or under the supervision of, the designated member of staff.

- 8.5 All cameras are kept in secure lockers and are put back at the end of every session.
- 8.6 Pictures taken and stored on the camera should be downloaded on to a school server as soon as possible.
- 8.7 School memory cards must not be used in other cameras: they should only be used in the camera to which they are assigned and the class teacher's desktop computer. They should be wiped at the end of each term.
- 8.8 Photographs of all our staff and governors are published on our website and noticeboards with their permission.
- 8.9 CCTV is used at the front gate, the outside area, and the ICT suite. CCTV footage is recorded and kept for security purposes only.
- 8.10 At St Aidan's we have no wish to prevent parents or carers taking photographs or films of the children in our care. We cannot, however, give permission for their publication. It is essential, therefore, that permission is obtained from the parents of all children appearing in images that are to be, for example, uploaded to the internet.

9 Cyber-bullying

Cyber-bullying takes place online through, for example, messaging apps and social networking or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (see also our Anti-bullying and Behaviour policies).

- 9.1 Class teachers discuss cyber-bullying with their classes, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This is done through all areas of the curriculum, particularly during Personal, Social, Health and Economic (PSHE) education lessons.
- 9.2 To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We ensure that pupils know how they can report any incidents and are encouraged to do so, whether they are a witness or the victim.
- 9.3 We will follow the processes set out in our *Anti-bullying policy* where cases of cyber-bullying are discovered. Where illegal, inappropriate or harmful material has been spread among pupils, we will use all reasonable endeavours to ensure the incident is contained.
 - The DSL will consider whether the incident should be reported to the police if it involves illegal material, working with external services if necessary.
- 9.4 All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- 9.5 We send information about cyber-bullying to parents to ensure that they are aware of the signs, how to report it and how they can support children who may be affected.

10 Working online

Children are supervised at all times, including break times, when working online.

10.1 In the unlikely event that any inappropriate material slips past our filtering system, children are taught to report it immediately to a member of staff. The subject leader for Computing (who keeps a record of all such incidents) and the Designated Safeguarding Lead will be informed and the site will be blocked manually. Inappropriate content is reported to Apple/Google.

11 Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to agree to the acceptable use of the school's ICT systems and the internet as set out in appendices 1, 2 and 3. Visitors will be expected to read and agree to these terms if relevant.

11.1 Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

11.2 We monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure compliance.

12 Use of work devices outside school

All members of staff must take appropriate steps to ensure their devices remain secure. This includes:

- keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- making sure the device locks if left inactive;
- not sharing the device among family or friends;
- keeping operating systems up to date – always installing the latest updates.

12.1 Devices must not be used in any way which would violate the school's terms of acceptable use. They must be used solely for work activities.

12.2 If staff have any concerns about the security of their device, they must seek advice from the ICT technician.

13 Education, advice and training

(More information about safeguarding training is set out in our *Safeguarding and child protection policy*.)

13.1 The Governing Body

Governors receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

13.2 The DSL and deputy DSL

The DSL and deputy DSL undertake safeguarding and child protection training, which includes online safety, at least every 2 years and continually keep themselves updated about online safety issues between annual reviews.

13.3 **Staff** (see section 15 below for more detail)

As part of their induction, all new members of staff receive training in safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

- All members of staff receive refresher training at least once each academic year as part of safeguarding training and get relevant updates as required (for example through emails, e-bulletins and staff meetings).

13.4 **Volunteers**

Volunteers receive appropriate training and updates, if applicable.

13.5 **Parents and carers**

This policy will be shared with parents and carers. Online safety advice is made available on our website, in information sent home and during parents' evenings.

- Concerns or queries about this policy can be raised with the Headteacher or any other member of staff.
- Any questions or concerns parents may have about online safety should be raised with the Headteacher and/or the DSL.

13.6 **Pupils** (see section 14 below for more detail)

Children are taught about online safety as part of the curriculum.

- Where necessary, teaching about online safety will be adapted for vulnerable children, victims of abuse and some pupils with SEND because a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach is often more suitable.

14 Pupils' online safety education

Aspects of online safety are taught across the curriculum. For example, the principles of respect and consent are emphasised during the Relationships, sex and health education lessons, a statutory part of the curriculum in all primary schools.

14.1 Children in **KS1** are taught to:

- use technology safely and respectfully, keeping personal information private;
- know where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

14.2 Children in **KS2** are taught to:

- use the technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour;
- identify a range of ways to report concerns about content and contact.

14.3 By the **end of primary school**, children will know:

- that people sometimes behave differently online, including by pretending to be someone they are not;
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online even when we are anonymous;
- the rules and principles for keeping safe online: how to recognise risks, harmful content and contact, and how to report them;
- how to critically consider their online friendships and sources of information and awareness of the risks associated with people they have never met;
- how information and data is shared and used online;

- what sorts of boundaries are appropriate in friendships with peers and others in a digital context;
- how to respond safely and appropriately to adults they may encounter online whom they do not know.

14.4 The safe use of social media and the internet will also be covered in other subjects where relevant.

15 Staff training

Training help staff:

- develop better awareness of the signs and symptoms of online abuse;
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up these risks;
- develop the ability to influence pupils to make the healthiest long-term choices and keep themselves safe from harm in the short term.

15.1 All staff will be made aware that:

- technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse;
- children can abuse their peers online through:
 - abusive, harassing, and misogynistic messages;
 - non-consensual sharing of indecent nude and semi-nude images and/or videos, especially in chat groups;
 - sharing of abusive images and pornography, to those who don't want to receive such content;
- physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

16 Dealing with infringements

It is the responsibility of all members of staff to be vigilant and report any concerns they might have to the Headteacher.

16.1 All concerns will be taken seriously, logged and investigated appropriately. Instances where the school is brought into disrepute may constitute misconduct or gross misconduct and disciplinary action may be applied (using the LA Disciplinary procedure).

16.2 Should there be any cause for concern, the Headteacher reserves the right to check images or other content stored on a mobile phone or other portable device belonging to a member of staff.

16.3 The DSL will be informed immediately if any inappropriate material is discovered and the LA will be contacted for advice about how to deal with it.

16.4 Any incident where inappropriate material might have been seen by a child at school must be reported to the class teacher, IT support, DSL and Headteacher.

16.5 We encourage children to discuss any anxieties they may have regarding inappropriate material they have seen outside school.

16.6 We provide advice to parents on the use of child friendly filters.

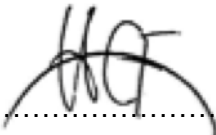
17 Review

The Care and Communication committee is responsible for the creation of this policy and its annual review.

18 Glossary

blog	Simple website
CCTV	Closed circuit television
DSL	Designated Safeguarding Lead
download	put material onto a computer
GDPR	General Data Protection Regulation
LA	Local authority
LGFL	London Grid for Learning
online	connected to the internet
PDF	Portable document format
upload	put material onto a website or blog
USB stick	Small device for transferring digital material
Wi-Fi	Wireless connection

Date of policy: JULY 2024

Policy ratified:  (Signature) 8th July 2024 (Date)

Review due: JULY 2025



Acceptable use agreement

EYFS and KS1 pupils

This is how I stay safe when I use computers:

I will always:

- ask a teacher if I want to use the computers;
- only use activities that a teacher has told or allowed me to use;
- take care of the computer and other equipment;
- ask for help from a teacher if I am not sure what to do or if I think I have done something wrong;
- tell a teacher if I see something that upsets me on the screen;
- know that if I break the rules I might not be allowed to use a computer.

Name:

Year:

Date:

Signed.



Acceptable use agreement

<p>KS2 pupils</p> <p>When I use the school's ICT systems (like computers) and get onto the internet in school...</p>	
<p>I will always:</p> <ul style="list-style-type: none"> • use the school's ICT systems and the internet responsibly and for educational purposes only; • only use them when a member of staff is present, or with their permission; • keep my username and passwords safe and not share these with others; • keep my private information safe at all times; • tell a member of staff immediately if I find any material which might upset, distress or harm me or others; • log off or shut down a computer when I've finished working on it. 	<p>I will never:</p> <ul style="list-style-type: none"> • give my name, address or telephone number to anyone without the permission of my teacher or parent/carer; • access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity; • open any attachments in emails, or follow any links in emails, without first checking with a teacher; • use any inappropriate language when communicating online, including in emails; • log in to the school's network using someone else's details; • arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.
<p>I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.</p>	
<p>Name:</p> <p>Year:</p> <p>Date:</p> <p>Signed.</p>	



Acceptable use agreement

All users

1. Personal Responsibility

As a representative of the School you will accept personal responsibility for reporting misuse of ICT resources to a member of the Senior Leadership Team. Misuse may come in many forms, but is commonly viewed as any information sent, received or viewed that indicates or suggests pornography, unethical or illegal activities, racism, sexism, inappropriate language or any use of which may be likely to cause offence.

2. Network Etiquette and Privacy

You are expected to abide by the generally accepted rules of network etiquette. These rules include but are not limited to the following:

- **Be polite.** Never send or encourage others to send, messages with abusive material.
- **Use appropriate language.** Remember that you are a representative of The School. Never use inappropriate language. Discussion of Illegal activities is strictly prohibited.
- **Privacy.** Do not reveal any personal information to anyone especially the home address or personal details of yourself or any others.
- **E-mail.** Electronic Mail (E-Mail) is not guaranteed to be private. Messages are screened for inappropriate material, and although in most cases this takes place automatically, your message may be individually screened. Messages supporting illegal or inappropriate activities may be reported to the relevant authorities.
- **Disruptions.** Do not use the ICT resources in a way that could be disruptive to others.
- **Other considerations.** Remember that humour and satire are very easily misinterpreted. Respect the rights and beliefs of others.

3. Services

The School makes no guarantees of any kind whether expressed or implied for the ICT service that is provided. The School denies any responsibility for the validity or accuracy of any information obtained by its internet services. We do not recommend or endorse the storage of data outside our network. If information is stored locally, for example on a laptops, the individual user is responsible for ensuring that their data is securely backed up.

4. Security

Security on our ICT services is very important. If you discover a security problem, please inform a member of the IT Department as soon as possible. Never demonstrate this problem to another user. All use of the ICT systems must be under your own username and password. Anyone found to be sharing accounts and passwords may have their access blocked. Any user identified as a security risk may have their access blocked and be subject to a disciplinary action.

5. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or any other networks that are connected to the system. This includes but is not limited to, uploading and/or creation of computer viruses, the wilful damage of computer hardware and deletion of data.

6. Electronic Mail & Messaging

An official email address will be provided to all staff members. This is the only email account which should be used to conduct work. Users are expected to use these services in a responsible



manner. The sending of any emails that breach the terms of the IT User Agreement will result in disciplinary actions. Bulk sending of email without prior permission (spamming) is also forbidden.

7. Monitoring

All users email and system accounts have been provided to them by the School and should not be considered personal accounts. They are loaned to the individual for duration of the time at The School in order to undertake specific activities. The School reserves the right to monitor activity, using both automated systems (scanning for file types, file content) and manually.

- Where there is sufficient reason to do so appropriate individuals will be granted access to the accounts.

8. Disciplinary Consequences

If the rules of the Acceptable Usage Policy are broken users will have their computer privileges removed, this includes logon abilities, access to email and access to the internet. Depending on the severity of the issue one or more of the above restrictions may be implemented.

If a Staff member breaches the Acceptable Usage Policy any incident will be reported to HR and the Senior Leadership Team for further action.

9. Acceptable Use: Workforce, Governors and Volunteers.

The use of ICT resources must be in support of the role perform for the School. You are personally responsible for this provision at all times when you use any of the ICT resources.

By using any School IT equipment after reading this ICT user Agreement means that you understand and accept these terms and conditions listed below Any breach of these conditions may lead to disciplinary proceedings.

- I understand that WhatsApp is/is not an approved communication channel for the school. As this is not a school-controlled platform, The school is not able to monitor or easily access the information held. This can cause issues if there were to be a Subject Access or Freedom of Information Request. Any existing WhatsApp group containing staff should not show any affiliation with the school via the name. The approved communication channels are school email/parent mail/Microsoft teams/google chat
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- My passwords will be “strong” in nature, and include capitals, lower case, number, and symbol and be of least 8 characters long. If I suspect it has been compromised, then I will change it immediately.
- I will ensure that I am the only one who uses my user Account and understand that anything undertaken while I am logged in, I will be held responsible for.
- I will not autosave my password or log in details for any of the School systems, as this negates the effectiveness of the password.
- I will lock my computer screen whenever I leave it unattended.
- I will ensure that all electronic communications are compatible with my professional role.
- If I receive a suspicious email, I will report it before clicking on any links, downloading any attachments or entering my user details. When I report it, I will not forward the email but send a screen shot.
- My personal social media accounts will not show a direct link with the School, and I understand that whatever I post can be seen, therefore if I am identifiable content will be of a professional nature.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.



- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue & Customs. Under no circumstances should the operating system or installed applications on any school-provided devices be modified by the user in any way.
- I will always check if I should be cc’ing bcc’ing recipients and that the correct email address, and attachment has been selected.
- I will transfer personal data by email securely e.g., using egress, or password protecting it. The password will be sent in a separate email.
- I understand that anything I write in an email or document about an identifiable person can be requested via a Subject Access Request and read by that individual. Therefore, would
- not write anything that I would not want that person to read, could bring the organisation into disrepute or is counter to the staff code of conduct.
- I will consider if the communications I send breach confidentiality or the Data Protection Act, by asking “should the recipient view this information”.
- I understand that I can cause a Data Protection breach by destroying or corrupting data and all data should be held in line with The School’s data retention schedule.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

I. I will support the School’s approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the organisation or its community’ onto my own social media platforms.

II. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Senior Leadership Team.

III. I will respect copyright and intellectual property rights and will ensure that any images that I use are not subject to copyright. These includes images found internet searches.

IV. I will ensure that my online activity, both in work and outside work, will not bring The School my professional reputation, or that of others, into disrepute.

V. I will alert the school designated safeguarding lead if I feel the behaviour of any child may be a cause for concern.

VI. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the designated Child protection lead.

VII. I will not use the School’s ICT systems for any commercial activities, such as work for a for-profit organisation.

VIII. When using personal devices please ensure that the device has anti-virus in place that has been updated to limit potential vulnerabilities.

IX. We appreciate that others may use the personal devices you access the system with however please ensure that you are the only person who can access your user Accounts and that you understand that anything undertaken while you are logged in, will be considered done by you.

X. I will only use school-approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff-only drive within school.

10. School Workforce Only

- I will only use the school’s LGFL email/ Internet / Intranet / and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher or Governors.
- I will ensure that personal data is kept secure and is used appropriately, whether in the school, or when working remotely.



- I will only access school resources remotely (such as from home) using the Insert method for remote access and follow e-security protocols to interact with them.
- I will not install any hardware or software without the permission of the IT Department.

11. Governors Only

- Governing Body documentation is stored electronically on Governor Hub or securely in hard copy in line with the School’s Document Retention Policy. Personal copies of documents should be retained in line with the school data retention schedule.
- Any information downloaded from the shared portal onto a personal device should be deleted upon the completion of the task, including from the temporary internet files.
- Only School-provided email accounts should be used for school business. This prevents subject access requests to personal email accounts and facilitates compliance with any email retention period. Please note, that this email account can be monitored by appropriate individuals if there is due cause.

Name:

Date:

Signed.