Whitefield
Academy Trust

Policy
Document

E-Safety Policy

Category: Leadership

Key Elements

This policy sets out what is expected of school leaders and staff across both schools in order to use ICT positively and to safeguard children and young people and to protect them from harm. Detailed guidance is available in a separate document. Implementation is monitored by the Senior Leadership Teams of both Schools and the e-Safety committee.

This version was reviewed on:
July 2020

Agreed by:
Directors

Due for Review:
July 2021

Table of Contents

1. Aims

This policy applies to all members of the Whitefield Academy Trust Community:

- Children and young people
- Staff
- Parents and carers
- Visitors
- Volunteers
- Students on courses

The Directors, Members of the Advisory Council and staff of the Whitefield Academy Trust recognise their duty to safeguard and promote the welfare of children and young people who are particularly vulnerable and to ensure that every effort is made to protect all children and young people from harm and to maintain confidentiality. The Trust aims to create and maintain a learning environment which is safe, caring, positive, and stimulating and which promotes the social, physical and moral development of all children and young people.

This is in line with the Trust's Mission Statement:

"Enjoyment, achievement and wellbeing for all".

It is the duty of the Trust to ensure that:

Every child and young person in its care is safe and to equip staff to keep themselves safe, and the same principles apply to the 'virtual' or digital world as apply to the school's physical buildings.

- We have robust processes in place to ensure the E-Safety of pupils, staff, volunteers and Directors
- We deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- We establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2019 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education; it is designed to sit alongside the Safeguarding Policy. Any issues and concerns with E-Safety must follow the school's safeguarding and child protection procedures.

This Policy document has been written to protect all parties by providing guidance on how to minimise risks and how to deal with any infringements.

It builds on the London Grid for Learning (LGfL) exemplar policy. It has been agreed by the Senior Leadership Teams of both Schools and approved by the Directors. It will be reviewed annually.

1.1. What are the main E-Safety risks today?

E-Safety policy and guidelines within the Academy Trust are designed to support children, young people and staff in the safe, positive and appropriate use of technology so that every effort is made to ensure that adults, children and young people experience the benefits of technology but are protected from:

- being exposed to illegal, inappropriate, distressing or harmful material (words and images)
- being exposed to material which may put them at risk of radicalisation or is otherwise at odds with the fundamental British values of democracy, tolerance and the rule of law
- experiencing harmful online interaction with other users
- behaving online in a way that makes them vulnerable to harm or causes harm to others

Whatever systems are in place it is not possible to guarantee that unsuitable material will never appear. These guidelines therefore also provide information on what to do when children or young people are exposed to inappropriate material.

All adults – staff, students and volunteers – must bear in mind the following key principles:

- All school policies apply in the virtual world as much as they do in the real world – for example the Code of Conduct applies to what is written on social media as much as to what is said in the staffroom
- Pupils and colleagues have a right to privacy and a right not to be spoken of unpleasantly or maliciously in any forum
- Staff are expected to maintain boundaries between their professional and personal lives, particularly in their relationships with pupils and their families
- All staff and volunteers have a duty to promote the reputation of the schools
- Staff are advised to protect their own reputation and career
- Staff and volunteers who work with vulnerable children and young people are seen as role models and need to be mindful of this in what they share with others

The E-safety policy and guidelines should be read alongside the following Trust policies:

- Safeguarding Children and Young People
- PSHE
- GDPR
- Use of CCTV

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (2019), in line with the **'Teaching E-Safety in school Guidance supporting schools to teach**

their pupils how to stay safe online, within new and existing school subjects' DfE Guidance, June 2019. and its advice for schools on:

- Teaching E-Safety in schools(2029)
- Preventing and tackling bullying (2017) and cyber-bullying: advice for Principal/Headteachers and school staff
- Relationships and sex education (2019)
- Searching, screening and confiscation (2014)

It also refers to the Department's guidance on protecting children from radicalisation (2015).

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in the Whitefield Academy Trust and the CEO and Senior Leadership Teams, with the support of Directors and Members of the Advisory Councils, are working to embed safe practices into the culture of the school. The responsibility for E-Safety has been delegated to the Vice Principal at Whitefield Schools who works in collaboration with the 's safeguarding team. Responsibility for e-Safety at Joseph Clarke School rests with the Headteacher who works in collaboration with the safeguarding team and the ICT Lead.

The Academy Trust has also established an e-safety committee to take oversight of key issues, to review the guidance provided in the light of ongoing developments and to monitor practice.

Adult members of the school communities must work within these policies whether in school, using school ICT equipment elsewhere, or working from home.

3.1 The Directors

The Directors have overall responsibility for monitoring this policy and holding the Principal/Headteacher to account for its implementation. Directors' key responsibilities are in accordance with Keeping Children Safe in Education 2019. This responsibility is delegated to the Directors in the Safeguarding Committee who receive termly reports on E-Safety as part of the Safeguarding report.

The Director who oversees E-Safety is Owen O'Regan.

3.2 The Principal/Principal/Headteacher

The Principal/Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The E-safety committee

The E-safety committee chaired by the E-safety lead will:

- meet termly
- oversee the implementation of the policy and E-Safety practice in school
- ensure the E-safety policy is implemented
- monitor the effectiveness of the E-safety policy
- have oversight of key issues and advise on practice
- report to Directors via the Safeguarding Committee
- ensure training and memberships are up to date

3.4 The Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) will ensure that all E-Safety concerns are dealt appropriately as safeguarding incidents in line with the Safeguarding Policy.

3.4 The E-Safety Lead

The E-Safety Leads are the Vice Principal at Whitefield Schools and the Headteacher at Joseph Clarke Schools who take lead responsibility for E-Safety in their schools. In particular they will:

- Support the Directors and the E-safety committee in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Ensure all staff are aware of the procedures that need to be followed in the event of an E-Safety incident, and that these are logged in the same way as any other safeguarding incident
- Ensure that any E-Safety incidents are logged and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Work with ICT Support Service and other staff, as necessary, to address any E-Safety issues or incidents and review the school's E-Safety system
- Update and deliver staff training on E-Safety liaise with other agencies and/or external services if necessary
- Provide termly E-Safety reports to the Directors as part of the Safeguarding Report.
- Liaise with the local authority and work with other agencies in line with Working together to safeguard children
- Communicate regularly with SLT and the designated safeguarding lead and E-Safety Director/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school
- Facilitate training and advice for all staff
- Ensure the school website meets statutory DfE requirements

- Work closely with the ICT support services to:
- Ensure appropriate filtering and monitoring systems are in place, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensure a full security check is conducted and monitored by the school's ICT systems on a regular basis
- Ensure access is blocked to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensure that any E-Safety incidents are logged using the school's safeguarding online systems and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school's behaviour and safeguarding policies

This list is not intended to be exhaustive.

3.5 Teachers

Teacher will:

- Read and agree to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Ensure their pupils remain safe online
- Monitor and be vigilant while pupils are using electronic devices
- Support their pupils, in line with their skills and abilities, to learn how to remain safe online.
- Support pupils to understand and follow the E-safety user agreements where appropriate
- Ensure pupils are taught, in line with their abilities, about E-Safety as part of the curriculum-

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers will:

- Read and follow this policy in conjunction with the school's main safeguarding policy and understand that E-Safety is a core part of safeguarding; as such it is everyone's responsibility to ensure children and young people remain safe when using the internet
- Know who the Designated Safeguarding Leads (DSL) and E-Safety Leads are
- Record E-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Sign and follow the staff acceptable use policy and code of conduct
- Carefully supervise and support pupils when engaged in activities involving online technology (including, extra-curricular and extended school activities if relevant)
- Prepare and check all online source and resources before using within the classroom
- Support pupils to follow their acceptable use policy, and support them in understanding the risks, where appropriate
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring pupils follow the school's terms on acceptable use (see appendix C in the Guidance document).
- Not use their phones while interacting with children and young people.

- Turn off/silence any smart watches while interacting with children and young people.

3.7 The Network manager/IT staff

- IT staff will:
  - Keep up to date with the school's E-Safety policy and technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
  - Work closely with the designated safeguarding lead / E-Safety lead / data protection officer to ensure that school systems and networks reflect school policy
  - Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
  - Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL, E-Safety leads and the senior leadership team
  - Maintain up-to-date documentation of the school's online security and technical procedures
  - Report online-safety related issues that come to their attention in line with school policy
  - Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
  - Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

3.8 Parents

Internet use in children and young peoples' homes is increasing rapidly. Unless parents are aware of the dangers, children and young people may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home.

The Trust seeks to work in partnership with parents in all areas of their children's education, to keep parents fully informed of the school curriculum, to share and celebrate progress and to discuss any concerns. These principles apply equally to children and young people's use of ICT.

The school will support parents to develop their knowledge and understanding of E-Safety through workshops and training.

Parents are asked to follow the school's policy on photos/videos taking on school premises (Appendix E-Guidance document)

Parents are encouraged to consult with the school if they have any concerns about their children's and others' use of technology.

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

- Think U Know: is a website with resources aimed at pupils of all ages, teachers, parents and carers. (www.thinkuknow.co.uk/). The website presents information about the safe use of internet through text and videos. The website also enables parents and children to report abuse.

- Grid Club: is a safe and appropriate website for children, teachers and parents to access curriculum resources as well as crafts, games. It is presented in a child friendly way with engaging animations and videos. www.gridclub.com
- The BBC's Chat Guide: www.bbc.co.uk/chatguide/ is a website providing advice for parents, teens and kids - available both online and in leaflet-form too

3.9 Visitors and members of the community

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

4. E-Safety tools

The Whitefield Academy Trust takes seriously its responsibility to ensure that ICT usage by all network users is responsible, safe and secure. The Whitefield Academy Trust has invested in tools to filter access to the internet and to monitor activity by all network users. Current systems include:

- London Grid for Learning filter systems which block access to websites identified as inappropriate. The Trust's ICT leads are able to control the level of filter;
- Impero reporting system which detects and reports access to potentially unsafe sites. Information related to potential breeches by children and young people is sent to the deputy heads of each school at Whitefield and to the Headteacher at Joseph Clarke School. Information related to potential breaches by adults is sent to the Headteacher at Joseph Clarke School and the e-safety lead at Whitefield Schools. A report of any significant breaches is made to the e-safety committee;
- School laptops that are used offsite have their hard drives encrypted
- Password protection for the school network, and for some individual files within it, to prevent unauthorised access to school data. File permissions are assigned granularly meaning users only have access to the information required for their jobs
- Guest users have no access to shared resources
- Machine user rights are locked down with only the ICT team able to make administrative changes
- In addition, the schools use CCTV cameras on site to enhance safety and security. See separate policy.

5. Educating pupils about E-Safety -The safe use of ICT

The Trust is developing a clear, progressive e-safety education programme. Children and young people are taught a range of skills and behaviours appropriate to their age and experience as follows.

Children and young people who have sufficient understanding are expected to take increasing responsibility for their own use of technology. They sign an acceptable use agreement form which is fully explained and used as part of the teaching programme (see Appendix C – Guidance document).

ICT in the 21st century has an all-encompassing role within the lives of children and young and adults. New technologies are enhancing communication and the sharing of information and supporting the Trust schools to provide a high quality of education.

E-safety is defined as the school's ability:

- to protect children and young people and staff from harm arising from inappropriate use of technology
- to educate children and young people and staff in the safe and appropriate use of technology
- to establish robust safeguarding mechanisms which will be used to support children and young people and staff where there is a risk of harm.

There are three areas of risk:

- **content**: being exposed to illegal, inappropriate, distressing or harmful material
- **contact**: being subjected to harmful online interaction with other users
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm.

Current and emerging technologies used in schools and, more importantly in many cases, used outside of school by children and young people and staff include:

- the Internet
- e-mail
- instant messaging
- blogs (an on-line interactive diary)
- podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- social networking sites such as Facebook
- video broadcasting sites such as YouTube
- chat rooms
- gaming sites
- music download sites
- mobile phones with camera and video functionality
- mobile technology (e.g. games consoles) that are 'internet ready'
- smart phones with e-mail, web functionality and cut down 'Office' applications.

As soon as they are allowed to access the internet independently, children and young people should be supported to understand the importance of safe and responsible use.

Useful e-safety programmes include:

- Think U Know: is a website with resources aimed at pupils of all ages, teachers, parents and carers. (www.thinkuknow.co.uk/). The website presents information about the safe use of internet through text and videos. The website also enables parents and children to report abuse.

- Grid Club: is a safe and appropriate website for children, teachers and parents to access curriculum resources as well as crafts, games. It is presented in a child friendly way with engaging animations and videos. www.gridclub.com
- The BBC's Chat Guide: www.bbc.co.uk/chatguide/ is a website providing advice for parents, teens and kids - available both online and in leaflet-form too.

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Creating a safe ICT learning environment includes three main elements:

- an effective range of technological tools;
- policies and procedures, with clear roles and responsibilities;

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps 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 the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that children and young people, who are able to, understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Directors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The Trust will also send information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's Safeguarding policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school 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, and will work with external services if it is deemed necessary to do so.

6.3 Upskirting

Upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education. Any such incidents will be dealt with on an individual basis in line with the Safeguarding policy.

Pupils involved in such incidents will be appropriately supported.

6.4 Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. All staff need to be aware of this guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the Safeguarding Team who will follow the full guidance.

6.5 Social Media/Online gaming

The Trust blocks/filters access to social networking sites and newsgroups unless a specific use is approved. Children and young people will be taught never to give out personal details of any kind which may identify them or their location or place personal photos on any social network space. Children and young people will be taught to deny access to unknown individuals and instructed how to block unwanted communication.

Video gaming is blocked in school. Children and young people, however, will be taught about the dangers of online gaming including explicit imagery and communication with strangers.

Social media breaches will be dealt with in line with the school positive behaviour policy (for pupils), safeguarding Policy or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the Trust will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the Trust may report it to the platform it is hosted on, and may contact the Professionals' E-Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and Director s are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

We will monitor the websites visited by pupils, staff, volunteers, Directors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

When appropriate, staff will collect the mobile devises from the pupils.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

Staff must not use online storage accounts e.g. google drives, other than those approved by the school, to store school and pupils related information

10. How the school will respond to issues of misuse

Where a child or young person misuses the school's ICT systems or internet, we will follow the procedures set out in the safeguarding policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, level of understanding of the child or young person and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the safeguarding policy /staff

disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The DSL will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All new staff will be briefed of E-Safety procedures as part of the safeguarding briefing before they come into contact with the children and young people.

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

The DSL /E-Safety Lead will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of E-Safety at regular intervals, and at least annually.

The Directors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the Trust and local area. Although many aspects will be informed by legislation and regulations we will involve staff, Directors, pupils and parents in writing and reviewing the policy (KCSIE stresses making use of teachers' day-to-day experience on the ground). This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Children and young people, where possible and appropriate, will help to design a version in language their peers understand. Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy would be immediately disseminated to all the above stakeholders.

The DSL will monitor logs behaviour and safeguarding issues related to E-Safety using the school's Safeguarding systems.

This policy will be monitored and reviewed annually by the E-safety Committee chaired by the E-safety Lead. After every review, the policy will be shared with the Directors.

13. Links with other policies

This E-Safety policy is linked to our:

- Safeguarding policy
- Positive Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

14. Handling complaints regarding e-Safety

The school takes all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is **not possible to guarantee that unsuitable material will never appear** on a school computer or hand-held device.

Staff and children and young people are given information about infringements in use and possible sanctions.

Complaints of cyber-bullying are dealt with in accordance with the School's Behaviour Policy.

Complaints related to safeguarding are dealt with in accordance with Schools' Safeguarding Policy.

Allegations of e-safety breaches by staff are dealt with in accordance with the Misconduct Policy.

The e-Safety Guidelines include more detailed information on what to do in response to e-Safety Breaches.

Appendix 1 - Whitefield Academy Trust

Acceptable Use Agreement Form

Staff and Directors - Acceptable Use Agreement Form

The school Acceptable Use Policy is designed to ensure that all staff are aware of their responsibilities when using any form of Information & Communications Technology within their professional role. All staff are expected to sign this policy and adhere at all times to its contents.

- I will comply with the ICT system security protocols and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all my electronic communications with parents are compatible with my professional role, and never via personal email / phone accounts / social networking profiles.
- I will not discuss school issues on social networking sites / web-blogs.
- I will not use my personal mobile phones or cameras whilst I am responsible for, or in the presence of children and young people
- I will not give out to pupils, my own personal contact details, such as mobile phone number and personal email address.
- I will only use the approved, secure email system(s) and LGFL tools for communications related to my professional role.
- I am aware that communicating with students / pupils via private email / SMS and social networking sites may be considered a disciplinary matter.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head of School/Headteacher and will be encrypted.
- I will not install any hardware or software without permission of the IT leader.
- I will not browse, download, upload or distribute any material of a pornographic, offensive, illegal or discriminatory nature. I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.
- I will not use any unauthorised devices or platforms to store information e.g. memory sticks, google drive
- I will only take or store images & videos of pupils and / or staff on school equipment and will only use them for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will match the content of material viewed on line to the age and understanding of individual children and young people; use bookmarks and 'favourites' to signpost appropriate sites and always preview websites before use and do not undertake searches where you cannot predict the outcome
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will immediately report any concerns to the e-safety Lead or the safeguarding team

User Signature

I have read the full school Acceptable Use Policy and I understand what is expected of me regarding my professional behaviours in the use of technologies.

Signature ..... Date .....
Full Name ..... (printed)
Job title . . . . . .

Appendix 2 - Staff receipt of E-safety policy and guidelines

I acknowledge receipt of the following documents:

- Whitefield Academy Trust E-safety policy
- Whitefield Academy Trust E-safety guidelines
- We have attended training on these documents and undertake to follow the guidance given to the best of my ability.
- I acknowledge that deliberate failure to follow the guidance in these documents may be dealt with within the Trust's disciplinary procedures.

Signed _____

Date _____

This policy is shared
via the school website:
www.whitefield.org.uk