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 Adopted on:
10/07/2017

Agreed by:
Directors

Due for Review:
July 2018

Table of Contents

E-Safety Policy Overview

1. Aims

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

- Children and young people
- Staff
- Parents
- Volunteers
- Students on courses
- Course tutors

The Directors, Members of the Advisory Councils 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.

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 Members of the Advisory Councils and Directors. It will be reviewed annually.

2. The safe use of ICT

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.

In addition the schools use CCTV cameras on site to enhance safety and security. See separate policy

The Whitefield Academy Trust takes seriously its responsibility to ensure that ICT usage by all network users is responsible, safe and secure. Creating a safe ICT learning environment includes three main elements:

- an effective range of technological tools;
- policies and procedures, with clear roles and responsibilities;
- a comprehensive e-Safety education programme for children and young people, staff and parents.

3. E-Safety tools

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;
- encrypted USB sticks to protect data in transit;
- password protection for the school network, and for some individual files within it, to prevent unauthorised access to school data.

4. E-safety policy and procedures

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 designated to the Vice Principal at Whitefield Schools who works in collaboration with each school's safeguarding team and the e-safety co-ordinator. Responsibility for e-Safety at Joseph Clarke School rests with the Headteacher who works in collaboration with the safeguarding team and the ICT Lead.

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

In doing this they need to take account of:

- safe use of e-mail;
- safe use of Internet including use of internet-based communication services, such as instant messaging and social networks;
- safe use of school network, equipment and data;
- safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- maintaining children and young people's privacy in line with parental wishes about the publication of information and photographs;
- appropriate responses to cyber-bullying;
- their role in providing e-safety education for pupils;
- appropriate use of digital communication, including social media, so as to avoid bringing the school into disrepute.

Staff must not use personal email, social media or personal mobile phones to contact children and young people and must not share personal contact details with children and young people or their families. They should not share personal contact details with children and young people or their families unless agreed by their Head of School for specific purposes e.g. when they are acting as befrienders.

Ex-pupils and their families should only make contact via professional email.

Staff must be very cautious when using social media, remembering that privacy can never be fully guaranteed. They must never share personal information about children and young people or colleagues and must never make negative remarks about the school, colleagues, pupils or parents.

Staff must not use School ICT resources for:

- social networking activities other than the Trust social media accounts and those approved by the Trust
- questionable activity – including the deliberate viewing of inappropriate material on the internet, DVD or other types of media
- illegally obtained software – this is all software that does not have a valid licence certificate for use in School

Staff who believe they may have clicked on any item inadvertently, such as links in phishing emails or buttons on websites that may be of a suspicious nature, should immediately seek advice from the school's e-safety co-ordinator or a member of the ICT support team.

The Trust has established an e-safety committee to take oversight of key issues to produce more detailed guidance and to monitor practice.

Whitefield School's **e-Safety Co-ordinator** is Evangelia Dimopoulou. Joseph Clarke School's **e-Safety Co-ordinator** is currently the ICT Lead Barry Carter (Katy Taylor from September 2017).

Whitefield School's **Designated Safeguarding Lead** is Laura Pease. Joseph Clarke School's **Designated Safeguarding Lead** is Isobel Cox.

The **Designated Director for Safeguarding** for Whitefield Academy Trust is Owen O'Rgan.

The e-Safety Coordinators keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as LGfL and The Child Exploitation and Online Protection (CEOP). The Vice Principal ensures that the CEO, Principal/Head Teacher, Senior Leadership Teams, Directors and Members of the Advisory Councils are updated as necessary and that decisions made by school leaders are communicated to the relevant people and implemented.

Directors and Members of the Advisory Councils need to have an overview of e-Safety issues and strategies at this school. The Academy Trust ensures that Directors and Members of the Advisory Councils are aware of local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following Trust e-Safety procedures.

This means

- fostering a culture in which children and young people feel able to report any bullying, abuse or inappropriate materials to a trusted adult

- maintaining vigilance in respect of those children and young people who are not able to protect themselves on line.

5. E-safety education

ICT use is widespread and all staff including administration and site staff are included in appropriate awareness raising and training. As a minimum:

- the e-Safety Policy and guidelines are issued and explained during induction as part of safeguarding training;
- staff are made aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential;
- staff that manage filtering systems or monitor ICT use are supervised by members of the Senior Leadership Team and have clear procedures for reporting issues;
- refresher training in safe and responsible Internet use within the school e-Safety Policy will be provided annually as part of safeguarding training. The ICT lead teacher and the e-Safety co-ordinator will advise individual staff on request.

It is important that all classroom staff feel confident to use new technologies for teaching and learning. Staff have opportunities to discuss the issues and develop appropriate teaching strategies within induction, continuing professional development and staff meetings.

If a member of staff is concerned about any aspect of ICT use in school, they should discuss this with their line manager or the e-safety co-ordinator to avoid any possible misunderstanding.

Some children and young people have a range of skills which enable them to access and make effective use of digital resources to support their learning. They are encouraged to understand the issues relating to safe and responsible use of ICT and adopt appropriate practices. The majority of children and young people at Whitefield will not have this ability due to their learning difficulties. They need to be protected by adults to ensure that they are not exposed to unnecessary risks.

Staff will check any materials used in class for appropriate content for their age and understanding of the group and for any issues which may affect particular children and young people.

Teachers only use materials in lessons which they have accessed in advance and checked for suitability. They ensure supervision when children and young people are allowed to search in an unstructured way during lessons or leisure time.

Teachers are able to monitor children and young people's use of the internet during lessons using Impero Software. They will make the children and young people aware that this is happening.

Some children and young people are very familiar with the culture of new technologies. They are involved in discussing the School e-Safety Guidelines through Student Council and will continue to be consulted as policies

and systems develop. Children and young peoples' perceptions of the risks may not be mature; the e-safety rules may need to be explained or discussed.

E-Safety is taught within the PSHE/SED curriculum for children and young people who can understand the key concepts. An e-Safety Programme of Study is under development. These children and young people need to learn how to control and minimise online risks and how to report a problem. Teachers plan the content and are also ready to respond to issues as they arise.

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.

6. Working with 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.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet is made available to parents through workshops.

E-safety issues are handled sensitively, and parents will be informed of any incident involving their child.

7. 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 t do in response to e-Safety Breaches.

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