# MILTON KEYNES EDUCATION TRUST

# WALTON HIGH

# Online Safety Policy

| | |
|---|---|
| Date approved | |
| Committee oversight | Learning, Teaching and Student Welfare Committee |
| Review date | September 2021 |
| Responsible officer | Ann Purser Pastoral Director |

| Revision | Status | Date | Author | Comments |
|---|---|---|---|---|
| 1.0 | Approved | Sept 2018 | A Purser | |
| 2.0 | Approved | 12.10.2020 | A Purser | Added section relating to 'blended learning' |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Contents

# 1. ONLINE SAFETY STATEMENT

This policy applies to all members of the Walton High community including staff, students, parents, visitors and community users. Online Safety is an area that is constantly evolving and as such, this policy will be reviewed on an annual basis.

Walton High uses technology and the internet extensively across all areas of the curriculum and the purpose of this policy is to ensure the whole school community is empowered with the knowledge to stay safe and free from risk. The policy also aims to ensure risks are identified, assessed and mitigated where possible in order to reduce any possible foreseeability of harm to students or staff or liability to the school.

# 2. POLICY GOVERNANCE (ROLES & RESPONSIBILITIES)

## Local Governing Body

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

- review this policy to ensure that the policy is up to date, covers all aspects of technology use within the school, ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents
- the Safeguarding governor to have overall responsibility for the governance of online safety at the school who will:
    - receive regular updates from the Principal and/or Designated Online Safety Lead in regards to training, identified risks and any incidents

## Principal

Reporting to the Governing body, the Principal has overall responsibility for online safety within the school. The day-to-day management of this will be delegated to a member of staff, the Designated Online Safety Lead (or more than one), as indicated below.
The Principal will ensure that:

- online 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 Online Safety Lead(s) has had appropriate CPD in order to undertake day to day duties
- all online safety incidents are dealt with promptly and appropriately

## Designated Online Safety Lead

The Designated Online Safety Lead will:

- keep up to date with the latest risks to children and young people whilst using technology
- familiarise themselves with the latest research and available resources for school and home use
- review this policy regularly and bring any concerns to the attention of the Principal
- advise the Principal and governing body on all online safety matters
- engage with parents and the school community on online safety matters at school and/or at home
- liaise with IT technical support and other agencies as required
- retain responsibility for the online safety incident log; ensuring staff know what to report and ensuring the appropriate audit trail
- ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with ICT Technical Support

- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- facilitate training and advice for all staff

## Designated Safeguarding Lead

The Designated Safeguarding Lead will:

- take day to day responsibility for online safety issues and have a role in establishing and reviewing the school online safety policies/documents
- liaise with relevant agencies
- be regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues arising from:
    - sharing of personal data
    - access to illegal/inappropriate materials
    - inappropriate online contact with adults/strangers
    - potential or actual incidents of grooming
    - cyber-bullying and use of social media

## ICT Technical Support Staff

ICT 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
    - windows (or other operating system) updates are regularly implemented and devices updated as appropriate
- any online 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 online safety officer and Principal
- passwords are applied correctly to all users regardless of age

## 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 Principal
- any online safety incident is reported to the Designated Online Safety Lead/ Designated Safeguarding Lead or in his/her absence to the Principal
- they adhere to the Staff Code of Conduct

## All Students

The boundaries of use of ICT equipment and services in Walton High are given in the student Acceptable Use Policy which can be found in the Student Diary; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour, Anti-Bullying and/or Child Protection and Safeguarding policies.

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

### Parents

Parents play the principal role in the development of their children; as such the school will ensure that parents can access the skills and knowledge they need to ensure the safety of children outside the school environment. Through Parents' Consultation meetings and school communications we will endeavour to keep parents up to date with new and emerging online safety risks, and will involve them in strategies to ensure that students are empowered to keep themselves e-safe.

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 before any access can be granted to school ICT equipment or services.

## 3. TECHNOLOGY

Walton High uses a range of devices including PCs and laptops. In order to safeguard students and prevent loss of personal data, we employ the following assistive technology:

- **Internet Filtering** – we use appropriate software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner
  The Designated Online Safety Lead and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Principal
- **Email Filtering** – email filtering is provided by Microsoft Office 365 in the cloud
- **Passwords** – all staff and students are unable to access any device without a unique username and password. With effect from insert date, staff will be required to change their passwords on a three monthly basis or if there has been a compromise, whichever is sooner
- **Anti-Virus** – All capable devices have anti-virus software. This software is updated daily for new virus definitions. IT Support are responsible for ensuring this task is carried out, and report to the Principal if there are any concerns

## 4. SAFE USE

### Internet

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

- to staff upon signing the Staff Acceptable Use Agreement
- to students upon them and parents signing the Acceptable Use Policy

The Behaviour, Anti-Bullying and/or Child Protection and Safeguarding policies may be applied to any misuse of the internet inside or outside of school.

### 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. Staff should familiarise themselves with the Email Usage Policy on Firefly.

Students are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of their intake year, initial, surname and a, e.g. John Smith who started in 2014 will be 14jsmith@mket.org.uk

The Behaviour, Anti-Bullying and/or Child Protection and Safeguarding policies may be applied to any misuse of the email inside or outside of school.

## Photos and videos

Storage and use of digital media such as photos and videos are covered in the Staff Code of Conduct.

## Children and online safety away from school

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to Children's Social Care and as required, the police.

Online teaching should follow the same principles as set out in the Code of Conduct.

Walton High will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- No one to one sessions, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household
- Any computers used should be in appropriate areas, for example, not in bedrooms
- The live class should be recorded so that if any issues were to arise, the video can be reviewed
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day
- Language must be professional and appropriate, including any family members in the background
- Staff must only use platforms provided by Walton High to communicate with students

Staff should record, the length, time, date and attendance of any sessions held unless this is done automatically and recorded as part of the platform being used.

## Social Networking

There are many social networking services available; Walton High is fully 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 Walton High and have been appropriately risk assessed:

- Walton High's Facebook page
- Walton High's Twitter account

Should staff wish to use other social media, permission must first be sought via the Principal who will ask the -Designated Safeguarding Lead and the Designated Online Safety Lead for advice before a decision is made. Reference should also be made to the Staff Code of Conduct.

SIMS must be consulted before any image or video of any child is uploaded to make sure permission has been given and GDPR regulations must be adhered to.
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".

All posted data must conform to GDPR and 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

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.

## Incidents

Any online safety incident is to be brought to the immediate attention of the Designated Online Safety Lead/Designated Safeguarding Lead, or in his/her absence the Principal. The Designated Online Safety Lead/Designated Safeguarding Lead will assist in taking the appropriate action to deal with the incident using the relevant policy (Behaviour Management, Anti-Bullying and Child Protection and Safeguarding) and fill out an incident log.

## 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. Should any member of staff feel they have had insufficient training generally or in any particular area this must be brought to the attention of the Designated Online Safety Lead or Principal for further CPD.

Online 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 students' learning.

Walton High has a clear, progressive online safety education programme as part of the Computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy
- to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- to understand how search engines work and to understand that this affects the results they see at the top of the listings (for older students)
- to understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand why they must not post pictures or videos of others without their permission
- to know not to download any files – such as music files – without permission

- to have strategies for dealing with receipt of inappropriate materials
- to understand why and how some people will 'groom' young people for sexual reasons
- to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline