FITZALAN HIGH SCHOOL
ICT STRATEGY & POLICIES FRAMEWORK

Contents:

Page number:

1. Introduction

This document is specific to Fitzalan High School and supports the ICT Protocol for Schools issued by the Cardiff Council, Schools and Lifelong Learning.

It concerns the use of all forms of information communication technology (ICT) in school, including: PCs; laptops; removable media devices (e.g. USB memory sticks, CDs, digital cameras, etc.); mobile phones; video conferencing; access to internet; email facilities; VLEs (Virtual Learning Environments).

The document applies to all staff based in school, it links to existing corporate policies that apply to all staff employed by Cardiff Council, and aims to provide clarity in the context of school based staff.

Its purpose, is to promote good use of ICT by school based staff and to protect staff. This document and all associated policies, will be reviewed annually by the Deputy Headteacher.

Rationale

Information technology gives pupils the opportunity to develop IT capability through their subjects. Within a rapidly changing world an awareness of information technology is vital for both career and personal development. IT is therefore, a feature of all areas of the curriculum and plays a significant role in creating a broad and balanced provision, supporting and enriching pupils' learning experiences.

Information and Communications Technology serves to enhance teaching and learning across all curriculum subject areas through the provision of up to date information and communications technologies supported by the contribution of well trained, highly skilled and motivated staff. A distinction is maintained within this policy between IT and ICT.

The implementation of this policy is the responsibility of the Headteacher, governors and all teaching staff. The pupil's entitlement is based upon the need to prepare pupils for a world demanding IT literacy.

2. Policies

Fitzalan High School ICT policies also include some adopted County Corporate ICT policies. These exist to direct staff on appropriate use of ICT. This section of the document makes reference to the policies and a summary overview of the content of each.

2.1 IT Security Policy

The Cardiff Council IT Security Policy provides a clear statement setting out the security management requirements and controls covering the use of Information Technology. The policy provides management direction and support for information security in accordance with business requirements, relevant laws and regulations, it underpins the security of information in the Council, and schools, and is a single reference point for identifying the necessary controls to ensure appropriate use of all aspects of Information and Communications Technology.

Within the context of a school:

The corporate policy makes reference to Government Secure Extranet (GCSx) / Government Connect / Code of Connections. This only applies to local government, i.e. the authority, and does not apply to schools directly, although it does have implications for accessibility of authority systems to school based staff. (N.B when staff access the Cardiff County Intranet website).

Within the school context, security organisation is the responsibility of the Headteacher supported by the Network Manager or SITS (Schools IT Support), depending on the level of support purchased from SITS through the Service Level Agreement (SLA).

In respect of security of electronic office systems and data, extra vigilance must be practiced in the classroom environment where unauthorised access to management information systems and email accounts in particular need to be guarded against.

The Schools & Lifelong Learning Service Internet Access Policy for Schools provides greater detail on expectations in schools than that provided in the internet facilities section of the IT Security Policy. In summary, the educational benefits of internet access far outweigh the possible risks and good planning and management will ensure appropriate and effective pupil use.

From a school perspective, when considering electronic file store and access it should be noted that no personal use / non educational use is permitted. Further detail on licensing for appropriate use of files such as music / video can be found in section 6.3 of this document, ‘Copyright and Software Licensing’.

From an educational perspective it may be appropriate to download material which may be deemed inappropriate in any other context, for example to use of racist / hateful materials such as Ku Klux Klan as an example of racism / hate in such lessons.

The school (Headteacher / governing body) reserves the right to withdraw or restrict / monitor access as necessary in the event of inappropriate use.

In respect of system access control, Fitzalan uses an acceptance notice at login for school staff.

Within the school environment compliance and audit remains the responsibility of the Headteacher / Chair of Governors. The school must maintain the list of essential records and retention periods, and also maintain an IT Asset Inventory, to include a software inventory. Schools IT facilities are provided for business and educational purposes, and any improper activity should be brought to the attention of the Headteacher.

2.2 Email Policy

The Cardiff Council Email Policy (Appendix 1) applies to all staff employed by Cardiff Council including temporary and agency staff. The policy sets out the obligations that all members of staff have when dealing with email messages. It covers two main areas of activity: the first concentrates on sending and receiving email messages and the second concentrates on managing email messages that have been sent or received. Staff must ensure that they are familiar with the content of the policy and use it as a point of reference when dealing with email messages.

Within the context of a school:

The introduction refers to possible legal action against the Council or individuals, within the school context the liability would lie with the school or individuals.

The corporate policy makes reference to Government Secure Extranet (GCSx) / Government Connect / Code of Connections. This only applies to local government, i.e. the authority, and does not apply to schools directly, although it does have implications for accessibility of authority systems to school based staff.

It is worth reiterating that extra vigilance must be practiced in the classroom environment, and any public access areas of a school, where unauthorised access to email accounts in particular need to be guarded against.

All staff staff use the secure council provided / approved email accounts (@cardiff.gov.uk or @fitzalan.cardiff.sch.uk) for all business / school related communication. It is essential that only these secure accounts are used when passing on sensitive or personal information. It should be noted that personal accounts such as hotmail are not secure.

It should be noted that SPAM software used in schools differs from that used in the Council, but the advice on receipt of unsolicited mail remains the same. If you don't recognise the sender and you believe the email to be SPAM then do not open and delete it from your inbox and your deleted items folder.

2.3 Mobile Phone/PDA Acceptable Use Policy

The PDA (Personal Digital Assistant) or mobile phone affords true business mobility, opening up a whole new world of opportunities for mobile working and a whole new world of risks. This policy sets out acceptable use of PDA's and mobile phones including security, risks, ownership, software and anti-virus, licences, e-mail and configuration.

Within the context of a school:

At present the school does not use PDAs

The PDA Acceptable Use Policy is being reviewed by corporate ICT to ensure it is applicable within the school context.

It should be noted that connection to corporate email facilities would require the use of a corporate device.

Fitzalan uses mobile phones for contact purposes on school trips. For these purposes, school issued mobile phones ought to be used. However, if it is necessary to use personal equipment these should not be used to capture or transmit personal data, for example photographs of pupils.

A Video Conferencing Acceptable Use Policy (AUP) has been developed to accompany this Policy. In summary, the AUP states the required system standards, security measures and appropriate use including seeking permission from parents, as well as recommendations for using video conferencing equipment safely.

2.4 Removable Media

It is recognised that staff occasionally use their own equipment such as memory sticks/flash drives. It must be noted that this is not advised and such usage is not permitted for the storage or transfer of **personal data** in line with GDPR and the Data Protection Act.

2.5 Remote Working

This section mainly covers the use of school portable computing devices (laptops etc.) away from the school.

Portable computing devices are provided to some members of staff to assist them in conducting official council / school business efficiently and effectively. This equipment, and any information stored on the portable computing devices, should be recognised as valuable organisational information assets and devices, including the software and data held on them, should be safeguarded appropriately.

Within the context of a school:

The corporate Remote Working Policy is being reviewed by corporate ICT to ensure it is applicable within the school context. Schools are advised to undertake a risk assessment regarding the use of portable devices, to determine whether encryption is necessary, further advice on this is available from Corporate ICT, but if there is a need to use the equipment for the transfer or processing of personal data, then it should be encrypted. At present, the use of portable devices at Fitzalan is limited to the senior leadership team and details are held in the School ICT inventory list and in the Information Asset Register.

2.6 Passwords

The level of password control will be defined by the Network Manager based on the value and sensitivity of the data involved, including the possible use of “time out” passwords where a terminal/PC is left unused for a defined period. Passwords protect access to all ICT systems, including “boot” passwords on PCs, particularly laptop/notebook PCs, as they are highly portable and less physically secure (it is acknowledged that the use of ‘boot’ passwords may not be feasible on Classroom PC’s). Ideally passwords should be memorised. If an infrequently used password needs to be recorded, this must be stored securely. Users are advised and regularly reminded about the potential risks of recorded passwords and given clear instructions on the safeguards to adopt.

Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data involved, e.g. ‘Master user’ passwords are more critical. Users should be instructed on appropriate techniques for selecting and setting a password. Passwords should be changed frequently to previously unused passwords. Some school systems have the capability to prompt or force the user, periodically, to select a new password. The Network Manager (under the direction of the Headteacher) should decide on the appropriate duration that users could leave their password unchanged. The typical period for password changes is every 90 days.

A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur. Users must not reveal their password to anyone. Users who forget their password must request that the Network Manager issue a new password. User ID and passwords for staff and pupils who have left the school are removed from the system within 1 month unless other arrangements have been made with the Headteacher.

Staff members should be regularly reminded of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems, remote gateway and/or learning platforms such as Moodle, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Within the context of a school:

Passwords should be-

- unique
- alphanumeric
- at least 8 digits in length
- changed at first logon (if temporary)
- regularly changed, at least every 90 days

Passwords should NOT be:

- written down/recorded without encrypted protection
- easy to guess
- shared with others (staff or pupils)

2.7 Disposal of Data and ICT Hardware

Prior to the transfer or disposal of any ICT equipment the Network Manager must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of The Data Protection Act to be met. School write-off procedures should be followed and all inventory lists updated. The School's disposal records will include:

- who authorised disposal
- confirmation that software and data has been removed
- the date that the item was disposed of
- how it was disposed of
- the name of the person/organisation that removed the disposed item.

The Data Protection Act requires that any personal data held on any obsolete machine be destroyed. It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently. Disposal of ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations.

2.8 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access secure ID), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: the Headteacher and the Facilities Manager.

3 Contact with Pupils Using ICT:

It is important that staff observe the professional boundaries and exercise the necessary caution when using ICT to communicate with pupils.

It is essential that staff avoid situations in both their work situation, and indeed outside of work, that could give rise to concerns about conduct or are in breach of the law. Therefore, staff should exercise extreme caution when communicating with pupils. This also applies to communications with colleagues about work related matters where professional policies and courtesies should be observed at all times.

The Council is clear that staff should not use any communication methods other than the school

provided accounts, including social networking such as Facebook/MSN and texting, to communicate with pupils. Staff will have email accounts established on the school's system and other communication tools that have been agreed within their schools, and these tools should be used for such communication. These tools are supported by audit trails which can help with responses to any complaints from parents, and indeed to protect the staff member when there is no evidence of inappropriate use.

Prior to being superseded by the Education Workforce Council, the General Teaching Council for Wales gave guidance on this issue:

> "A teacher should avoid situations both within and outside school which could bring them into conflict with the law or have an actual or perceived impact upon their status as a teachers;
>
> Teachers should ensure that:
>
> They fully comply with the LEA/school policies and procedures for the use of ICT facilities, email and the internet;
>
> They exercise caution in communicating with pupils including via email, text messaging, other media messaging or in sharing email addresses
>
> They exercise caution in relation to contact/web cam sites (for example, chat rooms, message boards and newsgroups)
>
> Teachers should ensure they do not:
>
> Have in their possession inappropriate materials/images in electronic or other format on school premises;
>
> Have in their possession at any time illegal materials/images in electronic or other format;
>
> Access inappropriate websites or download inappropriate material on school premises;
>
> Access at any time illegal websites or download such materials at any time or in any place"

It is important that all staff ensure that they are clear about these expectations to ensure the safeguarding of pupils as well as the interests of staff themselves.

4 e-Safety:

Cardiff Against Bullying and the Advisory Service have produced a Guide for Schools on Responding to e-Safety (Appendix 2). This comprehensive document details what e-safety is and why it is important, and looks at the roles of parents and staff.

5 Personal Use:

All staff should be mindful that guidance contained in this policy document is for staff protection and to promote responsible use of ICT.

5.1 Internet

It is understood that colleagues may occasionally need to make private use of the internet during the school day, for example at lunchtime. However, such personal use is to be kept to a minimum and must adhere strictly to the acceptable use of internet facilities detailed in the Council's IT Security Policy and the Internet Access Policy for Schools. The Headteacher reserves the right to determine when and if private use of the internet is excessive or obsessive during the working day.

5.2 Email

It is likely that employees will sometimes need to deal with private business during the course of

their working day. Appropriate, limited private use of email is permitted, provided such use is reasonable and does not interfere with work, nor take up more than a defined amount of time. Cardiff Council Email Policy details the conditions to be met for personal use of email.

5.3 Personal IT Equipment

As stated in the Council's IT Security Policy, and the school IT policy, the connection of any personal IT equipment to the council's (or School's) private network or a PC is not permitted. Personal equipment should not be used in the delivery of learning without explicit Headteacher agreement to do so.

5.4 Social Media

Guidance regarding the use of social media is detailed in the Cardiff Council's Social Media and Online User Policy (Appendix 3).

6 Control Systems / Compliance:

6.1 Filters

The Council employs internet content filter software to block access to certain internet categories which may contain inappropriate content. The internet content management categories for schools currently differ slightly from those applicable to the rest of the Council. Coaching pages are used for some sites on the corporate internet side, which give a warning rather than a block when trying to access a site or category of site. These coaching pages can also be useful in reminding people that they have spent a certain amount of time on a certain category of site. It has been agreed to introduce such coaching pages in the school setting to assist staff in ensuring appropriate internet usage. The filter categories will be reviewed and agreed annually by the ICT Policy for Schools Working Group, any requests for change must be submitted to the group through ICT.

6.2 Monitoring and Compliance

The IT Security Policy details the monitoring of system access and use, and compliance and audit requirements. Internet usage monitoring is carried out in schools for pupils through a supervisory role by teachers. We may wish to make arrangements to increase monitoring that takes place at a school level in certain circumstances, and further advice on this is available from SITS. It should be noted that centrally internet access across the school's network is logged, but it may not be possible to link back to an individual.

A breach or suspected breach of policy by a school employee, visitor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. For staff, any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure; policy breaches may also lead to criminal or civil proceedings. For pupils, reference will be made to the Relationships Policy and appropriate action taken.

Referral of any breaches should be made to the Headteacher, (and possibly the Data Controller, Governing Body and corporate ICT depending on the nature of the breach) linking into the Whistleblowing Policy, Disciplinary Policy, Complaints Process as appropriate. Investigation in the event of an incident may be criminal/child protection focused and dealt with in line with policy.

6.3 Copyright and Software Licensing

It should be noted that only lawful use of materials / software / equipment is permitted. The Council, on behalf of schools, coordinates the licensing applications for the following:

- Copyright Licensing Agency – photocopying and scanning of documents for use in school;
- Educational Recording Agency – making recordings for use in school;
- Phonographic Performance Limited – playing music recordings in school;
- Performing Rights Society – performing musical works in schools;
- Public Video Screening Licence – to show films in schools not part of the curriculum.

Similarly, any software used by school based staff must be appropriately licensed. Further information can be found at the following website: http://www.licensing-copyright.org/ .

7. Display Screen Risk Assessment

In accordance with the Display Screen Equipment Regulations 1992 as amended by the Health and Safety (Miscellaneous Amendments) Regulations 2002 any regular user of a Display Screen System must undertake a Display Screen Risk Assessment. A regular user is defined as a person who uses a Display Screen System in the work place for an extended period normally exceeding one hour.

7.1 Definitions

A Display Screen Equipment (DSE) is defined as a visual work station that includes a mounted PC, a laptop, touch screen system or any other Visual Display Unit (VDU).

7.2 Free Eye Tests And Spectacles

A regular DSE user as defined is entitled to a free eye test and prescription glasses if required are to be provided free of charge. Speak to the School HR department with regards to funding.

In line with this document all staff and school users must have read and signed the School's 'Acceptable Use of ICT Agreement' (found in the School Handbook).

Reviewed: October 2019

Next review date: June 2020