Exmouth Community College
Academy Trust

ICT and E SAFETY POLICY

Policy Details	Date
Written by	Graham Allen
Reviewed by	Adam Brealy
Ratified by	Curriculum Committee
Date agreed by Governors	12.03.24
Review Cycle	Annual
Review date	Spring 2025

TABLE OF CONTENTS

APPENDICIES

A. Introduction

This policy encompasses all aspects on Information Technology and electronic communications (e.g Mobile phones and Electronic Communication/Display/Recording devices). The policy operates in conjunction with other College polices including Safeguarding, Whistleblowing, Managing allegations against staff and the Staff Code of Conduct.

B. The Purpose of ICT

- The purpose of use of any form of ICT in College is to raise educational standards, to promote student achievement **in all subjects,** to support the work and development of staff and to ensure effective administration and management information systems.

- Computing is a part of the statutory curriculum and ICT is an essential tool for everyday living. Its use is highlighted in the aims of 'The Exmouth Curriculum'

- ICT gives access to learning and resources that reach beyond the boundaries of the College site. It enables
    - Access to online teaching and learning resources
    - Access to worldwide educational resources (e.g art galleries, museums)
    - Access to experts in many fields
    - Exchanges of views and information across different cultures
    - Professional development of staff
    - Collaboration across support services and outside agencies

As part of their learning at Exmouth Community College, students will be taught how to use ICT effectively and be able to understand what constitutes acceptable and effective use of the Internet.

C. Curriculum Use of ICT

C.1 ICT Contract

- Before using computers and ICT in the College, students must sign the 'College ICT Policy and Contract. Access to computers and ICT will be withdrawn if this is not received within a reasonable period (see **Appendix 1**).

C.2 Booking ICT Rooms

- All bookings for ICT suites must be made in advance by contacting the IT Helpdesk
- When a booking for a room has been made no swap of rooms must take place without informing the IT Helpdesk.
- Block bookings for ICT curriculum will be made by the Head of Computer Science.

C.3 Procedures for using ICT rooms with classes

- Staff should be aware of and use the document 'Lessons in ICT Rooms and Suites – 'WATCH LIFT MISS' (**Appendix 2**)
- Students should not be left unsupervised, given keys/pass cards to rooms or passwords to computers.
- If there is a fault, staff should report this to the IT Helpdesk in person, by phone or via email as quickly as possible, preferably by using the ITHelpdesk@exmouthcollege.devon.sch.uk email.
- Staff should be aware of additional security and health and safety issues regarding ICT.

C.4 Fault Reporting

- Faults should be reported as above.
- When reporting a fault, the machine number (blue asset sticker on the top of machine) should also be quoted.

- Fault logs will be monitored by the IT Manager and repairs will be carried out in the most effective way possible.
- Non ICT faults (e.g broken furniture) should be reported to the Estates and Facilities Helpdesk through the EVERY system.

C.5 New Hardware /Software

- All requests for new hardware/software must be made through the Head of Department and SLT Link.
- Staff should follow the procedures under 'Requesting New Hardware and Software Procedures' (**Appendix 3**)

D. Data Security

D.1 Principles

The College accepts and operates under the following principles

- Personal data shall be processed fairly and lawfully
- Personal data shall be processed for specified and lawful purposes
- Personal data shall be adequate, relevant and not excessive
- Personal data shall be accurate and where possible kept up to date
- Personal data must not be kept for longer than is necessary
- Personal data shall be processed in accordance with the rights of data subjects
- Personal data shall be kept secure
- Personal data must not be transferred to countries without adequate information

D.2 Key Staff

- Senior Risk Information Officer M Burrell
- Head of Computer Science J Quinn
- SLT Link to Curriculum ICT N Smith
- SLT Link to Technical IT M Burrell
- IT Manager A Brealy
- Personal data for staff G Morgan
- Personal data for students L Riggs
- Assessment data B Beaumont
- SEN data S Tigwell
- Medical data A Luxton
- Financial data M Burrell

D.3 Data Protection

- See **Appendix 4** for most recent information regarding data protection. See also the full Freedom of Information Policy.
- Any requests received under the 'Freedom of Information Act' and Data Subject Access Requests should be referred to M. Burrell.
- GDPRiS and DPIA's are used for recording due diligence has been exercised to ensure cloud hosted services the college use has a GDPR compliant policy, and that the college has agreed with these service providers what data can be processed.

D.4 Transferring Data

- All personal data should be stored safely and securely.
- **Personal data** refers to any information about someone. *(E.g. Student names, test scores, registers, addresses, electronic copies of staff appraisal reviews are all examples of personal data.)*
- Data held within the College network system are password protected
- Data held within the SIMs system are password protected
- Data contained within emails within College are password protected
- If staff send personal data via email to an external address OR transfer data via memory stick to an external computer, the data must be password protected. See Appendix 5 for procedures on securing data
- The College is aware of risks presented by memory sticks etc and encourages the use of MS OneDrive instead.
- Passwords should only be known by you. They should be strong, not easily guessed.
- Staff should consult with M Burrell or A Brealy before using any Cloud based resources that involve registering student names or any other personal details

E. E-Safety

- Any form of bullying using electronic means is unacceptable.
- **All members of staff have a responsibility to take reasonable measures to protect the safety of students on the internet and regarding electronic devices. To this end staff must enforce the mobile devices (phones) rules and must ensure that any web site found of an unfit nature available on our network should be reported immediately to the IT Manager for filtering.**
- Photos and videos of students may only be posted on authorised, College owned/managed sites (Website / Facebook / Instagram and Twitter). Staff should always adhere to permissions given by parents/carers/students under GDPR and students should not be named.
- **Students MAY NOT post pictures of staff, or set up sites in the name of a member of staff on any web page or site. Staff or students who become aware of such a site must inform a senior member of staff as quickly as possible.**
- When using Teams (or other remote meeting tools) students and staff must ensure that the location where the meeting is taking is place is of a suitable location, with no unsuitable images/backgrounds or other inappropriate materials visible during the call. In addition, staff must ensure the confidentiality of the call and follow the usual dress code. All other policies and procedures, as if the meeting (or lesson) was taking place face to face in College, must be followed.
- Any form of bullying of a college student (done at college/home or other location) using web based or other electronic applications and/or hardware is unacceptable and disciplinary action will be taken by the college. Mobile phones and electronic communication/display/recording devices are not allowed on the college site unless switched off: this is part of our policy to prevent e-bullying
- The College follows the advice given by the South West Grid for Learning in regard to 'sexting'. In the case of a reported or suspected incident staff should
    - Secure the device and ensure it is switched off
    - Use usual safeguarding procedures and alert a Designated Officer immediately
    - All incidents will be recorded, including details of actions taken or not taken, including the reasons.
    - The College would normally contact the police in the first instance
- Under no circumstances should staff give the number of a personal mobile phone to students. Staff organising visits should use a College phone, available from Donna French, in Accounts.
- If recording or photographing students for assessment or publicity purposes, staff should not use personal electronic devices. The College will provide equipment for this purpose.

- The “Acceptable Use policy” as published in Staff Handbook, Parent Guide and Homework Diary must be followed at all times.
- Finance staff who have access to any finance devices connected to the internet must follow the Payment Card Industry Security Standards - please see attached appendix The ICT and E-Safety Policy. It will be the responsibility of the Finance Manager to print this off and ensure that any member of staff who have access to any of these devices reads, signs and returns the appendix on an annual basis.

F. Email and Social Networking Sites

- Students are not allowed to access social networking sites from College.
- Students all have College email accounts which are monitored for safeguarding purposes, and students are taught about email.
- The College teaches students the dangers of using email and social networking sites and the College web site has guidance pages and appropriate links for staff/students and parents. All staff must encourage students to: Be E-Safe: protect your identity. THINK B4 U Click
- Staff use of email is detailed in the Staff Code of Conduct and **Guidance 9** of this policy.
- Staff should not have any existing student as a friend on any social networking site as this may compromise their professional standing and could lead to false accusations against them. Wherever possible they should also avoid having ex-students as friends (possibility of siblings / relatives still being at the College).
- Staff should be aware that social networking sites, despite security settings, are in the public domain and they should do nothing to endanger their own (or the College) professional standing (see also **Appendix 8**)

G. Acceptable Use

- A summary of the Staff Acceptable Use Agreement can be found in **Appendix 6**.
- Further guidance about Use and Participation in Social Media and Guidance on the Use of Emails can be found in **Appendix 8** and **9**.

H. Handling e-safety complaints

- Complaints of Internet misuse by students will be dealt with by a senior member of staff.
- Complaints about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the College’s safeguarding procedures.
- Students and parents will be informed of the complaints procedure.

I. Communication of Policy

I.1 Students

- Rules for safe use of ICT and ICT suites are printed on the College ICT policy contract signed by student and parent.
- Advice and e-safety guidance is available to students on the College website.

I.2 Parents

- Parents’ attention is drawn to the policy through the signing of the ICT agreement.
- Information regarding the policy is printed in the Parents’ Guide.
- Advice and e-safety guidance is available to parents on the College website.

I.3 Staff

- All staff will have access to a copy of the policy and its importance will be emphasised.

I.4 Governors

- Governors will receive a copy of this policy and will abide by e-safety procedures as set out in the policy and any additional protocols as agreed with the Headteacher

I.5 Visitors

- Visitors must abide by the e-safety procedures set out in this policy.
- Visitors will not be given unsupervised access to ICT resources.

J. Implementing and Monitoring the Policy

- All students and parents will be asked to sign the ICT agreement (**Appendix 1**).
- All staff and volunteers will be asked to sign the Acceptable Use Agreement (**Appendix 7**).
- The Governors will review the policy on an annual basis.
- The student contract / acceptable use agreement is kept under review.

This policy should be read in conjunction with the Equality Policy. No one will unlawfully be disadvantaged on the grounds of age, disability, gender re-assignment, marital or civil partnership status, pregnancy, maternity status, race, religion or belief, sex or sexual orientation.

This policy is also compliant with General Data Protection Regulation.

Appendix to the ICT and E-Safety Policy

This appendix is specific to Exmouth Community College because we use devices or systems in the businesses that are connected to the internet.

Secure and protect payment card data.

- Exmouth Community College collects or captures data and/or sensitive authentication data only where it really is needed.
- Exmouth Community College does not keep or store cardholder data after the initial transaction.
- Exmouth Community College does not keep or store sensitive authentication data after the initial payment transaction has been processed.
- Any cardholder data that Exmouth Community College has a need to keep is protected at all times. We make sure that cardholder data cannot be accessed by people that have no need to see or view the data.
- Exmouth Community College has a “clear desk policy” to make sure that people put away documents that may contain sensitive or cardholder data when not at their desk or work station.
- All cardholder data and sensitive authentication data collected is destroyed securely or erased once it is no longer needed for a business reason.
- Exmouth Community College destroy or erase cardholder data and/or sensitive authentication data using methods that make sure the information cannot be reconstructed or recovered.

Protect your systems by configuring them securely

- All unnecessary user accounts have been removed or disabled.
- Any default or “pre-set” passwords for user, administrative or system accounts have been changed.

Protect your business by enforcing a password policy

- All default and pre-set passwords on hardware, software and other systems and devices used by the business have been changed.
- Passwords are kept confidential. Users in Exmouth Community College know not to share the passwords.
- Users of the business systems, including staff, contractors and service providers, are required to choose strong passwords.
- Users are required to change their passwords regularly.
- Users of the systems know to avoid using the same password more than once.

Protect your business by controlling physical access

- The business premises and locations are kept secure. Only authorised personnel can access any non-public areas.
- Exmouth Community College has access controls in place to make sure that unauthorised persons do not have physical access to any of our business computers, servers or systems.

Raise Security awareness

- Exmouth Community College has an information security policy that lets the staff know what they need to do to keep customer’s payment card data safe.
- All employees have been brought through the company information security policy. They understand their role and responsibility they have in protecting customer cardholder data.
- Employees are periodically reminded of their security responsibilities.

Signed: ..... Date: .....

Appendix 1

Student ICT Acceptable Use Policy

Introduction

Digital technologies have become integral to the lives of children and young people, both within College and outside College. These technologies are powerful tools, which open up new opportunities for everyone. They can also stimulate discussion, promote creativity and raise awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- Young people will be responsible users and stay safe whilst using the internet and other digital technologies for educational, personal and recreational use.
- College systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk
- By agreeing to this policy, all students will have good access to digital technologies to enhance their learning

Acceptable Use Policy Agreement

For my own personal safety:

- I understand that I must use College systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
- I understand that the College will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone else may have access to it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

Equal rights to use technology as a resource:

- I understand that the College systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not use the College systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).

Security and integrity:

- I recognise that the College has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the College.

- I will turn any mobile device off while in College and at all times keep it completely hidden from view while on the College premises. I accept that the College will confiscate any mobile device if it is seen or heard on College premises.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any College device, nor will I try to alter computer settings.

- I will not use social media sites whilst in College or while using College equipment

Using the internet for research or recreation:

- I recognise that I must ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download copies (including music and videos)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

Appropriate behaviour:

- I will act as I expect others to act toward me.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will not take or distribute images of anyone without their permission.

- I understand that I am responsible for my actions, both in and out of College

- I understand that the College also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of College and where they involve my membership of the College community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the College network/internet, detention, exclusion, informing parents of unacceptable behaviour and in the event of illegal activities involvement of the police and or other appropriate bodies.

Student Acceptable Use Agreement Form

Please complete this part to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement and return to either your tutor or Dawn Howell in the ICT department.

If you do not sign and return this agreement, access to College systems and devices maybe withdrawn.

I have read and understand the above and agree to follow these guidelines when:

- I use the College systems and devices (both in and out of College)
- I use my own devices in the College (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of the College in a way that is related to me being a member of this College / eg communicating with other members of the College, accessing College email, website etc. This includes how you use social media.

Name of Student: ----------

Group / Class: ----------

Signed: ----------

Date: ----------

Parent / Carer Countersignature

Signed: ----------

Date: ----------

Appendix 3

REQUESTING NEW HARDWARE/SOFTWARE

Remember: all software/hardware changes/additions must be requested via the HOD/LINK

- Staff requests to install new hardware or software or change the way the school network operates must **get written consent** with the Head of Department/Dept ICT coordinator/Team Leader in the first instance. Do not contact the technical staff directly. The request should then be placed in the Department Development Plan by HOD after discussion with SLT. The IT Manager will produce a plan and priority order for approval by SLT/Headteacher
- Changes required but not in Academy Improvement Plan. Staff requests to install new hardware or software or change the way the school network operates must **get written consent** with the Head of Department/ Team Leader in the first instance. **Do not contact the technical staff directly.**

  The ICT Co Coordinator/Team Leader or HOD should then contact the IT Manager. Consequently there will be a meeting of IT Manager +HOD/Team Leader and, if possible, the LINK to manage the way forward (see below). Expenditure on ICT that is not in the school improvement plan (SIP) has not been budgeted for and therefore must have a funding source identified by this process.

- Procurement and Upgrades are Initiated by HOD/Link/School Development Plan (SDP), sequence below:

  1. Meeting with IT Manager/SLT
  2. Record form completed at that meeting (see below)
  3. Consider in light of whole college development/ICT infrastructure and SDP inclusion
  4. Proceed if positive and funds allow after costing by IT Manager. If funds do not allow record for action in next fiscal year
  5. When completed those at 1 above sign off project
  6. Jobs must be signed off on completion.

DEPT SOFTWARE UPGRADES

- The software must be evaluated by the HODHOD meets with IT Manager to discuss funding and installation needs
- The IT Manager instigates testing and installation and tasks technical team member with resolution of conflicts and installation problems.
- HOD instigates training of Dept in use of software
- .

COLLEGE SOFTWARE/HARDWARE UPGRADES

This is the responsibility of the IT Manager. College upgrades will be in response to educational needs and technical requirements where, for e.g. operating systems or applications are no longer supported and upgrading is necessary. Recommendations will be made to the Headteacher/SLT for approval. No upgrade/application removal will be undertaken without ensuring that the needs of the users are still fully met

Procurement Form

Delete as required: Software Hardware Upgrade Repair Email

Nature of request

Dept/Area Request instigated by: What is required?

Notes from meeting with HOD

How important to the teaching and learning?

Approved Yes/No IT Manager Signature: _____

_____

If approved for action next year. Priority: Low? Medium High?

Date of completion (if approved)_____

Signed off by _____ Date: _____

Signature_____

Freedom of Information

Reference: http://www.education.gov.uk/search/results?q=data+protection

By introducing on line reporting using SIMS.net or Gateway we are seeking to eliminate the pitfalls of the use of mobile storage devices. However guidance is given within the policy regarding security of data if it is transferred out of the secure College environment.

FOI Act Summary

Freedom of Information Overview

The Freedom of Information Act 2000 provides a general right of access to information held by Public Authorities (PA). Anyone can request information from a PA and has the right to be told:

1. Whether the PA holds the information, and
2. If it does, to be provided with the information

Key points:

- Anyone is entitled to make a FoI request for any information held by public authority (PA)
- Requests must be in writing, including email or FAX and can be given to any member of staff
- Requests need not mention FoI and PA cannot ask "Why?" the request is being made
- Information is anything held in a recorded form, eg paper files, loose papers, emails, electronic documents, photos, plans, maps, CCTV, videotapes, audiotapes, voice mails.
- Requests should be dealt with promptly and provide the information within 20 working days
- Requests are free if they cost less than £450 worth of effort. But disbursements (copying, postage etc) can be charged
- Above £450 pounds, PA can decline the request
- There are exemptions, e.g. personal data is covered by the Data Protection Act.
- Environmental information is covered by separate legislation. This is similar to FoI but only applies to information about land, air, atmosphere, water etc - Environmental Information Regulations
- In some cases the PA has to decide if it is in the public interest to disclose information even if there is an exemption
- If a PA is required to disclose information that might affect the rights and interests of third parties, consultation should take place with them first
- A PA must manage information properly and preserve all important records
- A PA must maintain a "Publication Scheme" which contains information routinely available without needing a formal FoI request.http://www.dca.gov.uk/foi/dftcp00.htm

The act can cover anything written down – including notes from meetings and emails.

Statutory right to know

The Freedom of Information Act creates a statutory right to know whether a public authority holds specified information, and if it does, to have that information communicated.

Public authorities will also be required to apply a publication scheme that gives details of information that it will provide proactively. It is likely that this requirement will come into effect first, followed, perhaps three months later by the requirement to provide information on request.

A public authority is any organisation or anyone acting on their behalf that carries out public functions, and includes such public bodies as local authorities, health, police, and central government. It will also include private companies and voluntary or charitable organisations if they are carrying out public functions on behalf of an authority.

What happens if the information contains details about people?

- Information that relates to identifiable individuals is exempt from the Freedom of Information Act. Any disclosures about people must comply with the Data Protection Act Principles, for example, obtaining their consent for information about them to be disclosed to the applicant.

Applicants who ask for a copy of personal information held about themselves must do so under the Data Protection Act and not the Freedom of Information Act.

- The Data Protection Act will be amended for public authorities in that anyone who makes a request to see a copy of information held about themselves will have the right to see a copy of information held in **unstructured manual files or records** as well as structured ones. This could include notes made by staff in a meeting, or comments jotted down on a file or post-it note about a person.

Are there any circumstances where information may be withheld?

There are several exemptions where information does not have to be provided under the Freedom of Information Act. These include circumstances where information:-

- has been provided under the common law duty of confidence
- was obtained during the course of a criminal investigation or an investigation that is required by law
- is held for the purpose of securing the health, safety and welfare of persons at work,
- is held for the prevention or detection of crime or the apprehension or prosecution of offenders,
- is held for the administration of justice,
- is held for the assessment or collection of any tax or duty or of any imposition of a similar nature,
- is subject to legal professional privilege in legal proceedings
- would prejudice the commercial interests of any person (including the public authority holding it).
- relates to or affects national security, police and intelligence services, defence of the realm or would prejudice relations between the UK and other countries

Most of these exemptions are covered by a public interest override. If the public interest in disclosure outweighs the public interest in maintaining the exemption, then the information **must be** disclosed. Even if information is covered by a duty of confidence to a person who provided it, a decision must be made as to whether releasing the information would be in the public interest. If it is, then the information must be provided.

Exmouth Community College
Privacy Notice – STUDENTS

Why are we giving this to you?

As your school we need to use information about you. We do this for a number of reasons. This form tells you what information we use about you and why we use it. It is very important that information about you is kept safe. We explain below how the school keeps your information safe.

If you want to know anything about what we do with information about you then please ask your teacher, or speak to your [parents/guardians] and ask them to contact the school. The school wants you to feel free to raise any questions at all.

We also have a person called the Data Protection Officer at the school. They can answer any questions you have about what the school does with your information. If you or your [parents/carer] want to speak to them, then you can do at:

Matt Burrell
Data Protection Officer
Exmouth Community College
Gipsy Lane
Exmouth
EX8 3AF

Email: Matt.Burrell@exmouthcollege.devon.sch.uk

Policy Statement

We are Exmouth Community College. During your time with us, we will use information that we gather in relation to you for various purposes. Information that we hold in relation to you is known as "personal data". This will include data that we obtain from you directly and data about you which we obtain from other people and organisations. We might also need to continue to hold your personal data for a period of time after you have left the school. Anything that we do with your personal data is known as "processing".

This document sets out what personal data we will hold about you, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

What information do we use about you?

We will collect, hold, share and otherwise use information about you set out in the boxes below:

• Name	• Telephone and email contact details	• Date of Birth
• Address	• Assessment information	• Details of previous/future schools
• Unique pupil number	• Behavioural information	• Language(s)

• Nationality	• Country of birth	• Eligibility for free school meals
• Photographs	• Attendance information	• CCTV images

We will also collect, hold, share and otherwise use some information about you which is "special category personal data" and we will take extra care to make sure that this is kept safe:

• Racial or ethnic origin	• Religious beliefs	• Special educational needs and disability information
• Medical / health information	• Genetic and biometric data	• Information relating to keeping you safe
• Sexual life	• Sexual orientation	• Dietary requirements

Where do we get this information from?

We get this information from:

- You
- Your [parents/carers], and other children's [parents/carers]
- Teachers and other staff
- People from other organisations, like doctors or the local authority for example

Why do we use this information?

We use this information for lots of reasons, including:

- To make sure that we give you a good education and to support you through this
- To make sure that we are able to address and support any educational, health or social needs you may have
- To make sure everyone is treated fairly and equally
- To keep you and everyone at the school safe and secure
- To deal with emergencies involving you
- To celebrate your achievements
- To provide reports and additional information to your parents/carers

Some of these things we have to do by law. Other things we do because we need to so that we can run the school.

Sometimes we need permission to use your information. This includes taking pictures or videos of you to be used on our website or in the newspaper. Before we do these things we will ask you or if necessary your parent/carer for permission.

Why do we use special category personal data?

We may need to use the information about you which is special (mentioned above) where there is a specific interest to do so for example health and social care purposes or to provide you with equal opportunities and treatment. We will also use this information where you have given us permission to do so.

There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests and where you are unable to provide your consent.

How long will we hold information in relation to our pupils?

We will hold information relating to you only for as long as necessary. How long we need to hold on to any information will depend on the type of information. Where you change school we will usually pass your information to your new school.

Who will we share pupil information with?

We may share information about you with:

- Other schools or educational institutions you may attend or require support from Local Authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes
- The Department for Education [and/ or ESFA] as required by the law
- Contractors, to enable them to provide an effective service to the school, such as school meal providers or external tutors

Keeping this information safe

It is very important that only people who need to use your information can see it. The school keeps you information safe by:

Keeping it on password protected computers

Having lockable offices and desk drawers

Taking great care of paper copies of personal data

Having very strong security for our computer network

Your rights in relation to your information

You can ask to see the information we hold about you. If you wish to do this you should contact

your form tutor who will help you.

You also have the right to:

- Object to what we are doing with your information
- Have inaccurate or incomplete information about you amended
- Ask us to stop doing certain things with your information in some cases

- Ask that decisions about you are not made using automatic systems

- Claim against the school in certain circumstances where you have suffered as a result of the school breaching your data protection rights

If you feel it necessary to do any of the above, you can speak with Mr Burrell. The school does not have to meet all of your requests and we will let you know where we are unable to do so.

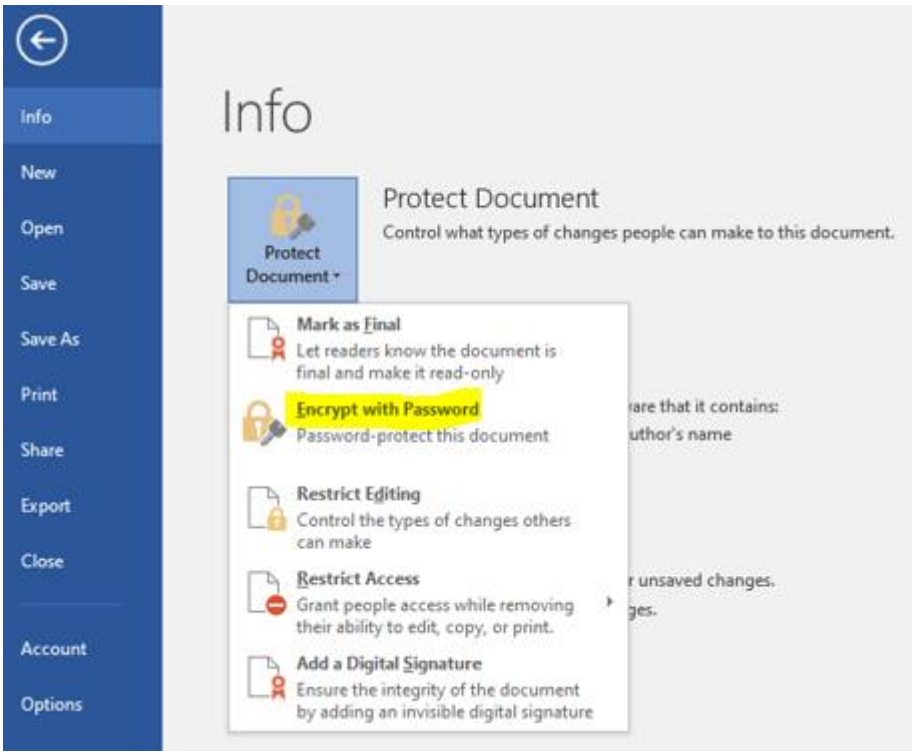
Concerns

If you are concerned about how we are using your personal data then you can speak with Mr Burrell or if necessary you or your parent/ carer can contact an outside agency - the Information Commissioner's Office who could also help at https://ico.org.uk/concerns/.

Encrypt your Microsoft Office file and set a password to open it

To encrypt your file and set a password to open it:

1. Click **File** on the menu and select the drop down arrow on **Protect Document**. Select **Encrypt with Password**.



2. In the **Encrypt Document** dialog box, in the **Password** box, type a password, and then click **OK**.

   You can type up to 255 characters. By default, this feature uses AES 128-bit advanced encryption. Encryption is a standard method used to help make your file more secure.

3. In the **Confirm Password** dialog box, in the **Re-enter password** box, type the password again, and then click **OK**.
4. To save the password, save the file.

Appendix 6

Acceptable ICT Use Summary for Staff

- Staff should recognise the importance of security of passwords and locked screens when not at PC. Work practice should follow the guidance given.
- Staff should be aware of the action to take when receiving suspicious emails/attachments/hyperlinks
- Staff should make appropriate use of their College email address and are responsible for the content of emails they send.
- Staff should follow the correct procedures for accessing files and using data
- Staff must be aware of safeguarding issues such as data protection and photos/phone numbers
- Staff have a responsibility to report issues / misuse to the IT Team and need to be alert.
- Staff inviting visitors should providing advance notice of outside agency use of network

Exmouth Community College Staff (and Volunteer) Acceptable Use Policy Agreement

College Policy

New technologies have become integral to the lives of children and young people in today's society, both within academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. **All users should have an entitlement to safe access to the internet and digital technologies at all times.**

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The College will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use College systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of the College digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, SIMS, RM Unify etc.) out of College, and to the transfer of personal data (digital or paper based) out of College (See Data Protection Policy)
- I understand that the College digital technology systems are intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to Adam Brealy (IT Manager) or Lisa Malton (Deputy Headteacher).

I will be professional in my communications and actions when using academy ICT systems :

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the College's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (eg on the College website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in College in accordance with the College's policies. (See ICT Safety Policy)
- I will only communicate with students and parents / carers using official College systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The College has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in College, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not register my College email address to conduct personal business (such as Ebay).
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will be responsible for backing up data on any external devices I use.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies. (See ICT Safety Policy)
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the College Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for College sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in College, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy
- I understand that if I knowingly fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Governing Board and in the event of illegal activities the involvement of the police.

I have read, understood and agree with the Staff (and Volunteer) Acceptable Use Policy Agreement:

Signed:..... Printed:..... Date:.....

Appendix 8

POLICY FOR USING & PARTICIPATING IN SOCIAL MEDIA

A.INTRODUCTION

Social media is the term commonly given to web-based tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests online. As the name implies, social media involves the building of online communities or networks to encourage participation and engagement.

This includes blogs, message boards, social networking websites (such as facebook, google+, twitter, Instagram, LinkedIn), content sharing websites (such as SnapChat, YouTube) and many other similar online channels.

This policy applies to all employees within ECC. It also applies to all governors and volunteers undertaking work on behalf ECC. Contractors and agency workers should also be made aware of this policy. These groups will be collectively referred to as 'individuals' within this policy.

All individuals' should be aware of their own conduct and behave in a manner which ensures and promotes acceptable behaviour in relation to their individual use of social media sites.

B. PRINCIPLES AND EXPECTATIONS

B.1. Other related policies

There are other policies and guidelines, including those listed below which govern employee behaviour in schools with respect to the disclosure of information online, including personal activities. All individuals within schools should make sure that they are familiar with this policy and those below:

- Staff Code of Conduct
- Disciplinary Policy for
- Teachers' Standards
- Equality in Employment Policy

B.2. Individuals are responsible for their own actions

ECC employees are encouraged to use the ICT systems they have at their disposal to enhance their work and learning opportunities for students' learning. The college, in turn, will expect its staff and volunteers to agree to be responsible users, exercising sound judgement and common sense.

Individuals should bear in mind that anything they post online, at work and at home, can potentially affect the reputation of the college and is ultimately the responsibility of the employee.

Individuals should ensure that privacy and security settings are set and used on all devices.

B.3. Be aware of working and personal lives overlapping

Online, an employee's personal and working lives are likely to overlap. Whilst ECC understands that many individuals use social media sites, it is important to remember that information/comments/images posted online originally intended just for friends and family can be forwarded on and might be viewed by students, parents and colleagues as well as members of the wider community. Be aware of your language and conduct while on these sites, the rules governing staff conduct, such as the Disciplinary Policy still apply.

Individuals should not accept pupils/students as 'friends' on social media sites.

If individuals have specific reasons for needing to communicate with students via a social media site they should first discuss this, with their reasons, with their line manager. Individuals must use their professional determination to set appropriate boundaries and if they are uncertain, to seek advice from the line manager **before** communicating with pupils/students.

Your conduct must not adversely affect the college's public image nor bring the college into disrepute. **This requirement extends to when individuals use social media sites outside normal working hours.** It is important that individuals should ensure that their security settings are set appropriately, including those on personal social media sites, so that individuals' own sites can only be accessed and used by those approved by that individual. Any information displayed on individuals' accounts are deemed to be their responsibility.

B.4. Participation in a public forum
Participation in a public forum must be professional. Individuals should make sure they always act in an honest, accurate, fair and responsible way at all times. Be aware of language and conduct while on these sites, the rules governing staff conduct, such the Disciplinary, Policy still apply.

When an employee participates in a public forum as part of their job they should specify their job title and ensure his/her line manager is aware of the discussion.

When an employee participates in a public forum as a private individual they must make that clear and only use their private e-mail address.

B.5. Consider carefully anything said/posted
Individuals are personally responsible for their words and actions. An individual must ensure that any confidential and/or sensitive information is not posted. Individuals must not make any derogatory, untrue or discriminating comments about the college, its pupils/students or other employees. Neither should any comments be made that are likely to affect the reputation of the college.

Confidential information, including information which is available to an employee due to the nature of their job, but is not in the public domain, should not be disclosed unless specific permission has been granted to do so.

If there is any doubt, do not post it.

B.6. Do not respond to negative comments posted online
If negative or disparaging comments about ECC its pupils/students and/or other individuals with connections to the college, are posted online or by third parties to try to spark negative conversations, individuals must not respond and should bring this to the attention of their manager.

B.7. Know that the Internet is permanent
As soon as information is published online, it is essentially part of a permanent record, even if it is removed or deleted later or attempts are made to make it anonymous. Information can be disseminated very quickly via social media and is virtually impossible to retract once it has been published; even if it has been online for only a short time, it may well have been picked up and copied and/or forwarded on by computers around the world.

C. STANDARDS OF BEHAVIOUR

ECC is committed to making the best use of all available technology and innovation to improve the way it works. However, individuals must use all forms of social media with extreme care, together with sound judgement and common sense. Failure to adhere to this policy and those policies listed at paragraph 1 may result in formal action within the Disciplinary Policy and other appropriate action in relation to governors, volunteers, etc.

In some circumstances, inappropriate communications may result in a police investigation.

D. USE OF SOCIAL MEDIA AT WORK

The use of school-owned laptops/computers/electronic devices to access social media sites for personal use is permitted where such use is restricted to lunch-breaks and usage is reasonable and appropriate.

Employees bringing personal electronic equipment in school, such as laptops/notebooks/hand held devices need to be aware that it is at the risk of the employees and the college will not be responsibility for the safekeeping of any such devices. Personal use of these devices must also be restricted to lunchbreaks.

Employees should note their contractual responsibility to devote their time fully to their work during paid hours. The Disciplinary Policy will be used to investigate any concerns regarding any employee found to be using electronic equipment for personal use during working hours, the outcome of which may lead to disciplinary action up to and including dismissal. As part of any such investigation, the college will check the employee's internet usage and will retain this information as appropriate.

E. SUMMING UP

Be aware of your association with ECC in online spaces. If identified as an employee or adult associated with the college, ensure your profile is appropriate and related content is consistent with professional expectations.

- Be aware of language and professional conduct.
- Be aware of issues such as libel, defamation and slander.
- Do not breach copyright
- Never share confidential or sensitive information.
- Inform senior management if participating online in a professional capacity.
- Individuals should alert senior management immediately if anything has been posted, inadvertently or otherwise, may cause issues for individuals and/or the college.

Appendix 9

Guidance on Use of Emails

Non-negotiable

Confidential information pertaining to students, parents or staff should **never** be viewed by unauthorised individuals. This could be through accidentally having the information projected on a screen (e.g details about FSM on a marksheet), overseen on a computer screen or a paper copy left visible.

Under no circumstances should a teacher plan lessons in such a way as to generate a window during which they can catch up on emails.

Moving Forward

As a result of consultation and feedback since the recent staff meetings the following four areas have been identified for clarification.

Protocol

As well as having a responsibility in accessing emails, staff also have a responsibility in what they send. The following are hypothetical examples of innocent mistakes that could be made:

- Confidential information being indicated in the subject line or visible pane in an email
- Creating an unnecessary sense of urgency by adding a red alert for something that is not urgent
- Using email instead of sending for instant support in the classroom

- The following clarification is given:
    - If the information required/to be shared is immediate (i.e during that lesson) runners should be sent directly to the teacher.
    - If the specific action /knowledge is needed by the teacher within 24 hours the 'Urgent' icon should be used (e.g a request to contact a parent)
- Confidential information about students should be recorded in CPOMS. **CPOMS must never be viewed when other students are in the room.**
- Staff should put confidential material in an attachment, not in the main body of the email.
- Staff should not display any information about students on a projector (including registers / marksheets /assessment data)

Pastoral Needs

There are occasions where staff need to alert colleagues or be alerted about a non-confidential issue regarding a child (e.g they have left a lesson late, they have gone to first aid).

- Staff to use professional judgement as long as this that does not contravene the areas already discussed above.

Enabling Teaching/Learning

While there are work arounds for teachers in terms of accessing resources there are times when email is the most effective way of ensuring students learning proceeds smoothly. Examples may be:

- The submission of cover work
- The use of an internet link that can be emailed to staff
- Submitting work requested to REACH/Internal/Study Centre
- Staff may access emails which have a direct impact on the quality of teaching/learning. If alternatives would create excessive extra work or would cause significant delay in providing work for students email can be accessed during lessons, provided that the areas above are not contravened.

Clarity on Conduct
The code of conduct will be used if a member of staff allowed any confidential information to be seen by unauthorised individuals or groups.

Reminder: CPOMS should never be viewed when other students are in the room